

We don't want to be their friends!

Zur Diskussion über Soziale Netzwerke

EA Bremen

Soziale Netzwerke, auch Social Media genannt, sind „eine Vielfalt digitaler Medien und Technologien, die es Nutzern ermöglichen, sich untereinander auszutauschen und mediale Inhalte einzeln oder in Gemeinschaft zu gestalten“ (Wikipedia). Soweit, so gut. Was aber bewegt eine_n dazu, „mediale Inhalte gemeinschaftlich zu gestalten“?

■ Nun, das ist zunächst einmal die recht einfache Benutzung von Chats, Blogs, Newsgroups und so weiter, die im Gegensatz zu den meisten anderen „alten“ Medien nicht nur den direkten Zugang zur Materie bieten, sondern eine_n dabei auch noch aktiv mitmachen lassen. Und so kann es gelingen, über diese Netzwerke nicht nur Kontakte mit Leuten zu pflegen, die man eben just über diese Medien kennengelernt hat, sondern auch mit längst verloren geglaubten Schulfreund_innen, Sandkastenkumpels und so weiter in Kontakt zu treten oder sich mit Gleichgesinnten aus der ganzen Welt immer und ständig auszutauschen.

Da man jedoch nur virtuell in Erscheinung tritt, bieten die Netzwerke noch andere Vorteile: Jede_r kann (zunächst!) selbst darüber entscheiden, welches Erscheinungsbild er/sie präsentieren möchte. Man kann die eigene kulturelle Identität gestalten: Du entspricht nicht den gängigen Schönheitsidealen? Kein Problem! Dank der virtuellen Welt

wird aus jeder/jedem eine schicke Punkrockerin oder der gefeierte Antifa-Held. Und auch den alten Schulfreund_innen kann man vorgaukeln, dass man statt dem beschissenen Job und den nicht vorhandenen realen Freund_innen so richtig das goldene Los gezogen habe. Mein Auto, mein Haus, meine Yacht mal anders: 200 Freunde bei Facebook ist die neue Marke, an der man sich messen kann. Dass die virtuelle Welt gerade denjenigen hilft, sich zumindest virtuell einzubringen, denen die direkte soziale Interaktion zum Beispiel aufgrund von Schüchternheit Angst macht, ist dabei ein Vorteil, der langfristig mit Vorsicht zu betrachten sein wird. Verschiebungen von Realität und eine zunehmende Individualisierung sind nur einige Folgen der virtuellen Konstruktion des Ichs.

Aber natürlich bieten Netzwerke auch andere unübersehbare Vorteile. Immer ist man über Alles schnell und ohne Zeitverzögerung informiert. Die Generation 2.0 möchte nicht warten, bis es am nächsten Tag in der Zeitung steht. Sie möchte mitgestalten und kann es auch. Was heute gebloggt oder getwittert wird, wird auch heute gelesen und kommentiert – und das weltweit. Ein paar flinke Fingerübungen auf der Tastatur und die ganze Welt bekommt es mit.

Virtuelles Leben, echte Daten

Erscheint man also virtuell als jemand anderes, funktioniert in der Realität die ganze Chose nur, wenn man zumindest einige „echte“ Daten angibt. Nur dann kann man die unbestreitbaren Vorteile der Sozialen Netzwerke in ihrer Gänze in Anspruch nehmen. Das bringt einige Gefahren mit sich. Und zwar nicht nur für dich – auch für Andere!

Dazu wollen wir im Folgenden etwas ausführlicher werden, wobei wir zwischen solchen Sozialen Netzwerken unterscheiden, die primär dem visuellen Austausch dienen, wie Youtube oder Flickr, und solchen, die vor allem, aber natürlich nicht ausschließlich, schriftliche Kommunikation und Messaging beinhalten wie Schüler und Studi VZ oder Facebook. Zunächst zu Letzteren.

Wenn man sich bei Facebook oder Myspace einen Account einrichten möchte, dann muss man zunächst einmal Daten angeben. Und auch wenn einem_r versichert wird, dass die Daten nach datenschutzrechtlichen Kriterien behandelt

werden, ist das nur die halbe Wahrheit. Daten werden nämlich nur nicht an Unbefugte weitergegeben, sprich an diejenigen, die keinen Account besitzen oder nicht gutes Geld investieren, um anhand deiner Profile ihre Werbung platzieren zu können. Der „Service“ der Sozialen Netzwerke ist für dich umsonst, die Betreiber_innen lassen sich die ganze Sache aber auf Heller und Pfennig bezahlen, ja machen sogar ein Riesengeschäft damit. Das bedeutet, dass deine Daten teilweise ungewollt veröffentlicht werden, sei es zugunsten anderer Nutzer_innen oder der Werbeindustrie.

Doch auch Verfolgungsbehörden profitieren von Facebooks Datenschätzen. Facebook hat sogar eine eigene Anwendung namens „Neoprint“ entwickelt, die den Behörden auf Anfrage ein handliches Informationspaket über Konteninhaber_innen zusammenstellt, das neben sämtlichen Profil- und Kontaktinformationen unter anderem Mini-Feed, Notizen, Freund_innenlisten (mit sämtlichen Facebook-IDs), Gruppenlisten und Nachrichten enthält. Auch Fotos – private wie öffentliche – werden Behörden zur Verfügung gestellt.

Einmal abgegeben ist es zudem wirklich schwer beziehungsweise unmöglich, das Ganze rückgängig zu machen. Das Netz vergisst so schnell nicht. Kontrolle über deine Daten haben also längst andere übernommen. Nicht so schlimm sagst du, steht eh nix drin. Die Wahrheit sieht auch hier leider anders aus.

Preisgegeben wird nämlich meist nicht nur der Name und das Alter, sondern es wird freiwillige Auskunft über Wohnort, politische Einstellung und Freund_innen erteilt, dezidiert gesagt, was man mag beziehungsweise „liked“. Viele posten auch, wen oder was sie gar nicht mögen, sei es der Stress mit Eltern, Nazis oder Polizei. Und selbst wenn du nichts über deine politischen Aktivitäten geschrieben hast, dann vielleicht deine Freund_innen, von denen dann auf dich indirekt verwiesen und damit auch über dich Auskunft gegeben wird. Und so lassen die auf den Sozialen Medien kreierte Netzwerke häufig Rückschlüsse auf reale Politzusammenhänge zu. Dazu sagt zum Beispiel Jonathan Chang, seines Zeichens Mitarbeiter der Datenforschungsabteilung bei Facebook: „Ist es nicht cool, dass wir die politischen Neigungen jedes Einzelnen in unserem

Datensatz von 500 Millionen Personen kennen?“¹ Das, wofür der Verfassungsschutz sonst einige Mitarbeiter_innen benötigt, wird ihm somit auf dem goldenen Tablett serviert.

Bilder und Daten unverschlüsselt frei Haus

Manchmal werden dann auch gar noch die entsprechenden Fotos mitgeliefert, auf denen die ganze Bande dann bei der letzten Demo zu sehen ist. In den seltensten Fällen wird sich die Mühe gemacht, diese dann zu verpixeln oder nur so rudimentär, dass es kein Computergenie braucht, um an die realen Daten heranzukommen. Im schlimmsten Fall wird die Info, um was es sich bei der Aktion handelt und wer wie dabei beteiligt war, gleich mitgeliefert oder in Private Messages kommuniziert, die wiederum auch nicht wirklich privat sind. Denn sie liegen unverschlüsselt auf den Servern der Betreiber_innen des Sozialen Netzwerks und können so immer an Verfolgungsbehörden weitergegeben werden.

Aber auch „private“ Fotos geben mehr über dich preis, als dir lieb sein sollte. Sie zeigen, wo du mit wem rumhängst, wie es da aussieht, wie du dich so kleidest und so weiter. Auch auf Partys werden immer wieder Fotos gemacht, die am Ende im Netz landen. Noch weniger als bei Bildern von Aktionen wird hier auf den Schutz der abgebildeten Personen geachtet. Wie uncool ist denn bitte ein verpixeltes Partyfoto? Gerade diese Bilder dienen Nazis und Polizei aber zur Aufdeckung von sozialen Strukturen und Zusammenhängen. Aus Ermittlungsakten geht hervor, dass Soziale Netzwerke gezielt durchsucht werden, um die Identität unbekannter „tatverdächtiger“ Personen ausfindig zu machen. Erst kürzlich erschien in der „Süddeutschen Zeitung“ ein Artikel, aus dem hervorging, dass die Polizei in Nordrhein-Westfalen in den letzten drei Jahren 3000 Straftaten im Internet aufdeckte. Schwerpunkte der polizeilichen Internetrecherche/Fahndung waren neben Kinderpornographie und dem Handel mit gefälschten beziehungsweise illegalen Medikamenten auch politische motivierte Straftaten².

Aber auch von anderer Seite droht

Gefahr: Nicht umsonst sind die Sozialen Netzwerke bei Arbeitgeber_innen so beliebt, um ein wenig mehr über den/die potentielle_n Kandidat_in für die begehrte Stelle zu erfahren. Und die schauen vielleicht zunächst nur einmal nach, ob kompromittierende Partybilder von dir existieren. Ob du ihnen aber auch die Möglichkeit geben willst, sich über dein politisches und privates Umfeld zu informieren, solltest du dir genau überlegen. Ganz andere Möglichkeiten der Datenanalyse haben dann die Mitarbeiter_innen der staatlichen Verfolgungsbehörden. Sie interessiert jeder Link, der von deinem StudiVZ-Account verzeichnet wird, und sie kommen spielend einfach an die vermeintlich verborgenen personenbezogenen Daten. So schreiben die Polizeidozenten Axel Henrichs und Jörg Wilhelm in einem Aufsatz in der Zeitschrift „Kriminalistik“ von 2010, Soziale Netzwerke seien „wahre Fundgruben für Ermittlungs- und Fahndungszwecke“.

Automatische Gesichtserkennung

Wie sieht es aus, wenn du soziale Plattformen wie Youtube nur bedienst? Vornehmlich geht es bei Plattformen wie Youtube, MyVideo, Flickr oder Picasa darum, Videos und Bilder auszutauschen beziehungsweise der Öffentlichkeit zu präsentieren. Dabei entwickeln sich diese Plattformen jedoch selbst immer mehr zu Sozialen Netzwerken oben genannter Machart. So gibt es auch hier Möglichkeiten „Freund_innen“ hinzuzufügen, eigene Favoriten zu verwalten und zu teilen oder Nachrichten zu verfassen. Im Hintergrund spielen sich noch weit komplexere Dinge ab. So weiß Youtube sehr genau, was für Videos einen außerdem interessieren könnten und Dienste wie Picasa können automatisch Gesichter erkennen – dazu aber später mehr.

Doch erst einmal zu vordergründigen Problemen: Immer mehr Menschen rüsten sich für Aktionen mit guten Film- und Fotokameras aus. Zusätzlich besitzt fast jede_r ein Fotohandy. Es entstehen flächendeckende Bilddokumentationen, die den Detailgrad der Überwachung der Bullen oft übertreffen. Diese Datenflut ist schon gefährlich, bevor sie überhaupt veröffentlicht wurde. Einzelne Kameras

können konfisziert und die Daten auf den Speicherkarten ausgewertet werden. Sich und andere davor und vor den Folgen zu schützen, ist in den seltensten Fällen realistisch. Noch schlimmer wird es dann, wenn die gemachten Bilder und Videos im Nachhinein veröffentlicht werden. Viele von ihnen finden ihren Weg unverpixelt ins Netz. Das ist eine klare Missachtung des Schutzes der abgebildeten Personen und endet zuweilen in Strafanzeigen und Gerichtsverfahren gegen Einzelne. In Berlin wurde zum Beispiel am 10. Juni 2009 eine Person zu 15 Monaten Haft verurteilt auf Grundlage eines bei Youtube eingestellten Videos.

Sicherlich ist ein Argument für das Filmen und Fotografieren, Übergriffe der Polizei zu dokumentieren. Doch die Bilder haben danach nichts im Netz zu suchen, sondern sollten an Soli- oder Antirepressionsgruppen weitergegeben werden, die sie sicher aufbewahren und für politische Arbeit verwenden können.

Das Problem der massenhaften Bereitstellung von Fotos hat noch eine weitere Dimension. Mit Gesichtserkennungsfunktionen, die heute jede_r_m zur Verfügung stehen, ist es ohne Weiteres möglich, schnell und sicher herauszufinden, wer mit wem zu welchem Anlass zusammen war. So ist es zum Beispiel mit der Software Picasa von Google möglich, Fotos nach Gesichtern zu durchsuchen. Ist ein Gesicht erst einmal einem Namen zugeordnet, ist Picasa dazu in der Lage, diese Person auf allen durchsuchten Bildern wiederzufinden. Eine eingeschränkte Veröffentlichung ist kaum realisierbar. Sind die Bilder einmal verteilt, können sie nicht wieder „eingesammelt“ werden. Wie schon gesagt wurde: Das Netz „vergisst“ nicht!

Die am Anfang erwähnten Funktionen der Bilder- und Videovorschläge erweitern die Problematik. Nicht nur die Menschen, die Videos oder Bilder hochladen oder auf diesen zu sehen sind, sind einer erhöhten Repressionsgefahr ausgesetzt. Auch das Anschauen von Videos und Bildern wird protokolliert und zu einem Interessen-Profil zusammengefasst. Dieses Profil ist zwar nicht öffentlich und verbleibt bei den jeweiligen Anbieter_innen, doch auch hier ist es denkbar, dass Daten an Verfolgungsbehörden

(1) Zit. nach Niklas Hofmann: „Unser Lastenheft. Was Facebook mit den Daten seiner Nutzer vorhat“, in: Süddeutsche Zeitung, 10. Januar 2011
(2) „Ins Netz gegangen“, Süddeutsche Zeitung vom 2. März 2011

weitergegeben und von ihnen verarbeitet werden. Gerade die Zusammenführung von Daten aus Sozialen Netzwerken wie Facebook und Youtube birgt ein großes Risiko. Es kommen detaillierte Persönlichkeitsinformationen mit Bildmaterial zusammen. Daten, für deren Ermittlung Verfolgungsbehörden viel Geld ausgaben – aber das müssen sie ja nicht mehr!

Staat und Wirtschaft reiben sich die Hände

Fassen wir also zusammen: Soziale Netze können vieles sein – Nachrichtenmedium, Kontaktbörse, Visitenkarte oder einfach eine Suchmaschine, um verlorene Freund_innen wiederzufinden. Sie sprechen die wesentlichen Bedürfnisse eines Menschen an, wie zum Beispiel das Bedürfnis nach Kontakt und das nach Zugehörigkeit. Kein Wunder, dass diese Netzwerke sich nicht gerade über mangelnden Zulauf beklagen müssen. Wer in einem sozialen Netzwerk ein Profil anlegt, sollte sich jedoch darüber im Klaren sein, welche Gefahr in ihren/seinen Angaben steckt. Weltweit werden ständig Daten aus dem Internet kopiert, archiviert und/oder weiter gegeben. Wirtschaft, Werbung und auch der Staat reiben sich die Hände, zumindest wenn es darum geht, in möglichst großem Umfang personenbezogene Daten zu sammeln.

Soziale Netzwerke sind im Alltag fest und allgegenwärtig verankert. Sich ihnen komplett zu entziehen wird immer schwieriger beziehungsweise ist kaum noch realisierbar. Umso wichtiger ist es, sich der möglichen Gefahren dieser Plattformen bewusst zu werden und gewissenhaft und sensibel mit seinen eigenen und den Daten anderer umzugehen. Das heißt konkret: Je weniger (wahre) Daten, desto besser! Hierbei muss klar sein, dass wahre Daten auch von anderen geschaffen werden können, zum Beispiel durch Benennungen auf Fotos. Ist es wirklich notwendig, in allen sozialen Netzen einen Account zu besitzen?

Es ließe sich auch auf Alternativen wie zum Beispiel Crabgrass zurückgreifen: Deren Betreiber_innen sind selbst Teil emanzipatorischer Zusammenhänge, legen großen Wert auf die Anonymität und Datensicherheit ihrer Nutzer_innen und sind bereit, gegen Datenschutzverstöße etwa durch staatliche Behörden entschlossen vorzugehen.

Generell sollte vor dem Anlegen eines Accounts reflektiert werden, wofür und zu welchem Zweck diese Plattform genutzt werden soll. Ein Account für politische Arbeit sollte nicht mit privaten Fotos und weiteren personenbezogenen Daten gefüllt werden! Beim Veröffentlichen von Fotos müssen mindestens Gesichter so unkenntlich gemacht werden, dass eine

Rekonstruktion im Nachhinein nicht mehr möglich ist (der gute alte schwarze Balken ist hier beispielsweise immer noch die sicherste Variante). Bedenkt aber hierbei, dass auch andere Merkmale (Piercings, Tattoos, Schuhe und anderes) von Bedeutung sein können!

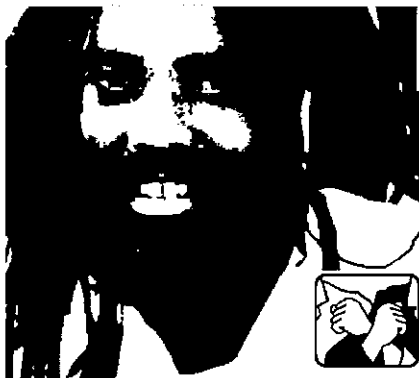
Der politische Bezug beziehungsweise Inhalt hat in deinem persönlichen Profil nichts zu suchen. Denkt bitte daran: Wenn ihr als Politgruppe Facebook und so weiter nutzt, heißt das auch immer, dass ihr Links zwischen euch und Einzelnen provoziert!

Politische Arbeit heißt, dass Verantwortung für andere und für Strukturen übernommen werden muss – das gilt insbesondere auch für Soziale Netzwerke! Wir haben es in diesen mit einer Verknüpfung von personenbezogenen Daten und Informationen in einer weltweiten Öffentlichkeit zu tun, bei der die Verschränkung von Privatem und Politischem eine andere Qualität bekommen hat. Niemand würde beispielsweise im „realen“ Leben auf die Idee kommen, zur Polizei zu gehen und dort ein wenig über sich selbst, das private Leben und das politische Anliegen zu plaudern. Und genau das sollte in Sozialen Netzwerken auch nicht passieren.

ANZEIGE

RAGE AGAINST THE DEATH MACHINE

Free Mumia Now!!



Neuer Solidaritätssampler für Mumia Abu-Jamal. Doppel-CD mit über 30 Bands:

28 years of injustice

13,- Euro. Bestellungen über: Jump Up-Bremen, Matthias Henk, Postfach 110447, 28207 Bremen, E-Mail: jumpup@t-online.de, www.jump-up.de

Herausgeber: Rote Hilfe e.V.

