Ist Datenschutz uncool?

Dr. Alexander Dix,
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Der Chef von Facebook, Mark Zuckerberg, hat gerade in einem Interview erklärt, die weltweit größte Online Community passe sich den geänderten sozialen Normen nur an. Als er mit Facebook in Harvard begonnen habe, hätten sich die Leute gefragt, warum man überhaupt Daten über sich ins Web stellen sollte. Mittlerweile würden die Menschen immer mehr Informationen über sich preisgeben und mit anderen teilen. Dem entsprächen die neuen Facebook-Grundeinstellungen. Zuckerberg ist offenbar der Meinung, Datenschutz sei nicht mehr so richtig zeitgemäß. Er hat übrigens auch 300 eigene Privatfotos öffentlich zugänglich gemacht, unter denen sich versehentlich auch private Aufnahmen seiner Freundin befanden.

Tatsache ist aber, dass Facebook mit diesen Grundeinstellungen seinen Nutzern praktisch vorschreibt, was sie wem zu offenbaren haben. Wer nicht aufgepasst hat, dessen Daten waren seit Dezember 2009 von heute auf morgen für alle Facebook-Mitglieder sichtbar und nicht nur für die „Freunde" des jeweiligen Users. Um das zu ändern, mussten die User Einstellungen ändern. Wem das zu umständlich war oder wer die geänderten Voreinstellungen überhaupt nicht mitbekommen hatte, der musste damit leben, dass das hochgeladene Profil einschließlich Foto und anderen Informationen wie Hobbys, Musik-Vorlieben etc. Leuten offenbart wurden, für die sie ursprünglich nicht gedacht waren. Offenbar hatte auch der Gründer von Facebook nicht mitbekommen, was die geänderten Voreinstellungen bedeuteten, denn er sperrte wenig später einige private Bilder seiner Freundin in seinem Profil, die durch die Umstellung für alle Facebook-Nutzer zugänglich geworden waren.

Das führt zu der Grundfrage, worum es beim Datenschutz überhaupt geht. „Datenschutz" ist ein veralteter Begriff, der so klingt, als gehe es um den Schutz von Daten um ihrer selbst willen. Worum es wirklich geht, hat der Chef von Google, Eric Schmidt, in schöner Offenheit so formuliert: „Wenn es etwas gibt, dass Sie andere nicht wissen lassen wollen, hätten Sie es vielleicht gar nicht erst tun sollen." Mit anderen Worten: wenn es nach Google geht, sollte kein Mensch mehr irgendwelche Geheimnisse vor irgendwem haben. Er sollte sich so verhalten, dass alle es wissen können (denn mithilfe von Google werden alle es wissen).

In einer solchen Gesellschaft will aber niemand leben. Letztlich brauchen wir den Datenschutz auch und gerade im Web 2.0, um uns frei bewegen zu können. Datenschutz schützt keine Daten, sondern das Grundrecht jedes einzelnen Menschen auf Verhaltensfreiheit. Verhaltensfreiheit gibt es nur, wenn jeder selbst entscheidet, was mit seinen Daten geschieht. Was hat Google mit Facebook zu tun ? Die

Dr. Alexander Dix
wurde am 2. Juni 2005 vom Abgeordnetenhaus zum Berliner Beauftragten für Datenschutz und Informationsfreiheit gewählt. Dr. Alexander Dix, LL.M., geb.1951, ist seit Juni 2005 Berliner Beauftragter für Datenschutz und Informationsfreiheit. Zuvor war er sieben Jahre Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg. Er ist Vorsitzender der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (international auch bekannt als "Berlin Group") und Mitglied der Artikel 29-Gruppe der Europäischen Datenschutzbeauftragten. Das Studium der Rechtswissenschaften in Bochum, Hamburg und London schloss er mit dem Grad eines Master of Laws an der London School of Economics and Political Science ab und promovierte 1984 zum Dr. jur. an der Universität Hamburg. Er begann seine Tätigkeit beim Berliner Datenschutzbeauftragten 1985 und war von 1990 bis 1998 dessen Stellvertreter.

Suchmaschine von Google durchsucht auch Online Communities, wenn diese es nicht verhindern (was möglich ist). Von niemandem kann aber verhindert werden, dass „Freunde“ oder andere Mitglieder der Community ein Suchprogramm („crawler“) im Inneren der Community starten, um dann massenhaft Daten von der Plattform abzusaugen und ins offene Internet zu stellen. Das widerspricht zwar den Nutzungsbedingungen der meisten communities, ist aber weder strafbar noch technisch mit Sicherheit auszuschließen. Das ist in den vergangenen Monaten mehrfach passiert und hat zu erheblicher Unruhe unter Usern geführt, weil sie dieses Risiko nicht gesehen haben (sie wurden von den Betreibern auch nicht darauf hingewiesen).

Die Behauptung, Datenschutz werde gerade von jungen Menschen als uncool empfunden, ist falsch. Meine eigenen Erfahrungen mit Jugendlichen, die sich mit dem Thema beschäftigen, belegen etwas anderes. Es mag sein, dass Jugendliche heute etwas anderes unter Datenschutz und Schutz der Privatsphäre oder der Persönlichkeitsrechte verstehen. Aber sie erwarten gerade, wenn sie sich in einem sozialen Netzwerk tummeln, ein bestimmtes Maß an Intimität und Schutz vor allgemeiner Beobachtung. Mit dieser Erwartung werben Plattformen wie Facebook und StudiVZ geradezu. Allerdings wird diese Erwartung immer wieder enttäuscht, weil die Betreiber (vor allem Facebook) den Nutzern vorschreiben, was mit ihren Daten passiert. Das ist alles andere als datenschutzgerecht. Es kommt auch vor, dass User sich nicht um die vorhandenen Einstellmöglichkeiten kümmern, die bestimmte soziale Netzwerke durchaus anbieten, um den Schutz der eigenen Profildaten zu verbessern.

Worauf sollte man achten, wenn man soziale Netze nutzt ?

1. **Sich genau ansehen, welche Einstellmöglichkeiten ein soziales Netz bietet, welche Informationen in punkto Datenschutz gegeben werden.** Je weniger Einstellmöglichkeiten eine Plattform hat und je spärlicher oder unverständlicher die Informationen zum Umgang mit Nutzerdaten sind, desto weniger vertrauenswürdig ist der jeweilige Anbieter. Man sollte sich auf anderen Plattformen umsehen, ob sie besser sind.

2. **Die vorhandenen Einstellmöglichkeiten sollte man gleich zu Beginn nutzen, um die eigenen Profildaten möglichst nur den „Freunden“ zu zeigen, die man sich ausgesucht hat.** Auch wenn man dies tut, muss man damit rechnen, dass Daten aus dem eigenen Profil – evtl. unter Einsatz von „crawler“-Programmen oder im Einzelfall – kopiert und ins offene Internet exportiert werden, wo sie auch für künftige Arbeitgeber oder andere sichtbar sind. Wer das cool findet, muss sich nicht darum kümmern, die anderen sollten genauer überlegen, was für Daten und Bilder sie hochladen. Auch für sog. „Apps“, das sind kleine Online-Programme von Dritten, sollte man die hoffentlich vorhandenen Datenschutzeinstellungen genau prüfen. Denn in der Regel kann auch der Anbieter eines solchen Fremdprogramms auf die zugänglichen Daten zugreifen. Oft werden aber Daten – möglicherweise verdeckt – zugänglich gemacht, die z.B. für ein einfaches Online-Spiel gar nicht notwendig sind.

3. **Möglichst unter Pseudonym im sozialen Netz auftreten.** Man muss sich zwar bei der Registrierung gegenüber dem Betreiber online identifizieren, kann sich aber dennoch anschließend einen passenden Spitznamen aussuchen. Jeder hat das Recht, einen Spitznamen in der community zu verwenden. Betreiber, die das untersagen, verstoßen gegen das Gesetz.

4. **Wenn man sich überhaupt in sozialen Netzen anmelden will, sollte man mehr als nur ein Netz nutzen.** Wie in der realen Welt hat man dann die Möglichkeit, verschiedenen „Freundeskreisen“ verschiedene Teile des eigenen Lebens mitzuteilen. **Es müssen und sollten gerade nicht alle alles über mich wissen.** Außerdem kann man in verschiedenen Netzen noch mehr interessante Leute kennenlernen.