24. Gert Egle: Facebook - Meine Ohrmarke "gefällt mir" - nicht (www.teachsam.de, 4.10.2011, gekürzt)

Dieser Spion lauert praktisch überall, wenn man auf eine Webseite kommt. Ganz oben oder ganz unten, manchmal auch irgendwo mittendrin. (...) Ja, eigentlich will er sogar, dass man ihn entdeckt, solange man nicht weiß, was er wirklich im Schilde führt. „Gefällt mir" heißt er und lädt jeden zum Mausklick auf seine äußere Hülle ein, die eine zweite, die verborgene, zur Täuschung umgibt.

Er schleicht sich ein in die affige Gefallsucht der Menschen und gaukelt den Selbstverliebten auch noch vor, Beachtung zu finden. Als werde einem wirklich einmal Gehör geschenkt mit dem, was einem gefällt oder eben auch nicht.

Facebook ist es mit dem ominösen Gefällt-mir-Button inzwischen gelungen, Millionen von Webseiten zu „verseuchen", und hat damit im Gegenzug Millionen neuer, werbewirksamer Daten von überwiegend ahnungslosen Websurfern „erschlichen". Denn, was die meisten nicht wissen: Wer zuvor schon einmal die Webseite von Facebook besucht hat, hat sich damit auch Facebook verkauft.

Wie auch immer er dort hingelangt ist, der Online-Krake hat ihm bei seinem Besuch einfach unbemerkt ein „Ei" ins eigene Nest gelegt. Cookies nennt man die kleinen Dinger, mit denen ein Webseitenbetreiber immer wieder erkennen kann, ob ein Rechner mit einer bestimmten IP wieder auf eine bestimmte Seite kommt. Ohne dass es der Besucher einer Seite merkt, wird sein Rechner mit einem Cookie, einem kleinen Textprogramm markiert, das es sich auf seinem Rechner erst mal bequem macht.

Kommt der Besucher dann wieder, kann er von dem Bertreiber der Webseite damit identifiziert werden. So weit so gut, aber es kommt noch schlimmer: Die Markierung des Rechners mit einem Cookie und alle damit gesammelten Daten werden einfach an andere Interessenten verkauft. Diese bleiben natürlich nicht untätig und schaffen durch die Verknüpfung mit weiteren u. U. ebenso gekauften Daten einen „Mehrwert", indem sie ein möglichst genaues digitales Abbild der Nutzer anstreben, das sich dann richtig zu Geld machen lässt.

Auf diese Weise „verwandelt sich der Bürger in ein durch und durch maschinenlesbares Wesen", wie Manfred Dworschak im Spiegel vom 10.1.2011 schreibt.

Das besagte Facebook-Cookie ist ein Späher der übelsten Sorte im Netz. Was ein Facebook-Mitglied im Netz treibt, entgeht ihm sowieso nicht. Aber, wer aus guten Gründen nicht dazugehört, fällt doch auch nicht auf den ominösen Knopf herein. Und: Wer dennoch darauf klickt, sollte wissen, was er tut, oder? Weit gefehlt! Wer das Facebook-Cookie einmal auf dem Rechner hat, ist in seinen Fängen.

Er wird nämlich von Facebook identifiziert, wenn er auf eine Seite im Internet gelangt, wo der unscheinbare Gefällt-mir-Knopf irgendwo platziert ist. Zwei Jahre lang, so sagt jedenfalls das Landeszentrum für Datenschutz Schleswig-Holstein, spioniert das Facebook-Cookie so vor sich hin, wenn man zwischenzeitlich, was sich ja oft gar nicht vermeiden lässt, nicht wieder einmal auf der Facebook-Seite gelandet ist. Und das soll alles mit rechten Dingen zugehen?

Eigentlich kann einem nur schwindelig werden, wenn man einmal ernsthaft darüber nachdenkt. Es gibt fast unendlich viele Möglichkeiten, mit denen heutzutage das Verhalten des einzelnen registriert und bewertet werden kann. Allen voran mit Cookies, die das Nutzerverhalten registrieren, dann mit Mobiltelefonen, die fortlaufend Lokalisierungsdaten erzeugen, ganz zu schweigen vom so genannten Geomarketing, bei dem Wohn- und Aufenthaltsorte mit allen möglichen Sekundärinformationen verknüpft werden, „vom Durchschnittseinkommen über das Alter bis zur Kaufkraft" (Schaar 2009, S.223).

Das amerikanische „Wall Street Journal" hat dazu einen interessanten Versuch gemacht. Ein Testcomputer musste dazu 50 besonders populäre Websites wie Yahoo, Ebay oder MSN nacheinander aufsuchen. Danach hat man einfach nur gezählt und festgestellt, dass auf dem Rechner, sage und schreibe, 3.180 Spähdateien, meistens Cookies, gespeichert worden waren. (...)

Na wenn schon, sagen hernach nur wenige, die mit solchen Daten konfrontiert werden. Denn spätestens dann sollte einem klarwerden, was Dworschak so treffend beschreibt: „Was für das Schaf die Ohrmarke, ist das Cookie für den Menschen. Es macht ihn identifizierbar. Wer ihm über Wochen oder gar Monate hinweg auf der Spur bleibt, erfährt immer mehr über seine Lebenslage, kann immer besser seine Absichten vorausberechnen - stets mit dem Ziel, dem erhofften Kunden, die aussichtsreichste Werbung zuzuspielen. Quasi als blinkendes Pünktchen auf den Radarschirmen zahlloser Verfolger bewegt sich der Mensch, beständig beobachtet, markiert und anderswo wiedererkannt."

Solche Ohrmarken rufen mittlerweile auch Politik und Datenschützer verstärkt auf den Plan, aber meistens sind ihnen die Hände gebunden. Es gibt so gut wie keine rechtliche Handhabe gegen die Späher, wenn sie ihren Sitz außerhalb Deutschlands oder Europas haben.

Hier müssen u. sollen bi- u. multinationale Abkommen helfen. Wenn sie einmal geschlossen sind, müssen sich freilich auch alle daran halten. Aber auch das ist derzeit noch Wunschdenken: Das im Jahr 2000 zw. der EU u. den USA geschlossene so genannte „Safe-Harbor-Abkommen" z. B., das den personenbezogenen Austausch von Daten auf eine legale Grundlage stellen soll, wird von den USA immer wieder unterlaufen. Sie halten sich einfach nicht daran, dass es danach amerikanischen Unternehmen im Prinzip verboten ist, in Europa gesammelte Daten in Länder weiterzuleiten, deren Umgang mit den Daten nicht den europäischen Normen und Standards entsprechen.

Aber mit den virtuellen Ohrmarken wird eben Geld gemacht, und zwar viel Geld. Mit der Marke im Ohr wird jeder zu einer Handelsware mit einem von der Genauigkeit des digitalen Abbilds abhängigen Wert, das hinter dem Rücken des einzelnen verschachert wird. Der Daten-Deal von Facebook mit dem Shopping-Riesen Amazon hat, wie COMPUTERBILD (10/2011) gemeldet hat, einen handfesten Skandal verursacht. Was angeblich nur auf der US-Seite von Amazon möglich sein soll, macht überdeutlich, was passiert, wenn sich zwei Datenkraken paaren. Auf der Amazon-Seite in den USA findet sich nämlich seitdem eine Schaltfläche namens „Connect with Facebook", also „mit Facebook verknüpfen". Wer darauf klickt, öffnet sein eigenes Facebook-Konto (sofern er eines hat).

Klickt man weiter, werden von einem kleinen Programm (App) die eigenen Profildaten an Amazon übermittelt und dazu noch die entsprechenden Daten aller Facebook-Freunde. Diese werden, versteht sich, darüber nicht informiert. Denn u. U. würden sie sich gar von ihrem Freund bei Facebook schnöde verraten fühlen, wenn dieser Amazon zu Daten wie Name, Geburtsdatum, Wohnort, Fotos, Hobbies, Lieblingsfilme und -bücher usw. Tür und Tor geöffnet hat.

Und das wäre dann der Anfang vom Ende des sozialen Netzwerkes. Vielleicht wäre das auch ein guter Anfang. Was im realen Leben nämlich wirklich wehtut und oft zu Tränen rührt: Freunde zu verlieren, ist in der digitalen Welt nur eine Frage eines oder einer Reihe von Mausklicks. Und das geht auch bei Facebook. „We do not trust you anymore, Mr. Zuckerberg! Your dumb fucks"[1] - Geben wir unsere virtuellen Ohrmarken einfach zurück. Schön wär's.

1) Ironische Anspielung auf Zuckerbergs frühere Antwort auf eine Frage nach der Herkunft von Daten: „They trust me, dumb fucks." (Sie vertrauen mir, die dummen Idioten.)

Aufgabe:

Analysieren Sie den vorliegenden Text.