

01.11.2017 - An den Rand notiert

Bist du schon ein «Target»?

von Rolf Euler

Wir haben uns in der Informatik an große Zahlen gewöhnt: Millionen (etwa Megapixel), Billionen (etwa Terabyte Speicherkapazität), Billionen (etwa Petaflops Rechenkapazität) und größer ? da muss die Finanzwirtschaft sich noch strecken. Nun müssen wir uns wieder an kleine Einheiten gewöhnen: Mikro (Millionstel) und Nano (Milliardstel) beim sogenannten Targeting.

Mikro- und Nanotargeting ist die Errungenschaft der Informationstechniker, aus großen Datenmengen durch Strukturierung und Profilierung auf kleinste Mengen von Teilnehmern bis hin zu Einzelpersonen herunterzuschließen. Diese Möglichkeiten wurden im Zusammenhang mit der US-Präsidentenwahl breit diskutiert, weil die Sorge bestand, die Wahlen ? oder allgemein Entscheidungen ? könnten manipuliert werden.

Targeting ist das gezielte Ansprechen von Personengruppen durch Information und Werbung. Diese Personen haben durch ihre Internettätigkeit, ihr Kaufverhalten mit Payback- und Kreditkarten, ihre Suchmaschinennutzung, ihren Facebookauftritt oder andere Datenspuren ein bestimmtes Profil in den Datenbergen, welche mithilfe von intelligent konstruierten Algorithmen durchsucht werden. Diese Profile werden von der Werbeindustrie verwendet, um Kaufentscheidungen mit personalisierter Werbung zu beeinflussen. Dies nutzen seit längerer Zeit auch politische Parteien, um Wahlentscheidungen für ihr Programm oder ihre Kandidaten zu beeinflussen.

Vor den Bundestagswahlen haben daher Wissenschaftler untersucht, was gemacht werden kann und welche Ergebnisse zu erwarten sind. Dabei beschränkten sie sich ? aufgrund der in Deutschland strengeren Datenschutzgesetze als in den USA ? auf öffentlich zugängliche Facebook-Profile, das heißt Daten, die die Facebook-Nutzer «freiwillig» von sich einstellen. Das sind dann etwa «Likes» (der Daumen-hoch-Button) auf den Seiten der politischen Parteien, die sich weitgehend problemlos Einzelpersonen zuordnen lassen mithilfe der ID der Nutzer bzw. ihres Account-Namens, der oft mit dem Klarnamen übereinstimmt oder leicht herauszufinden ist.

Mit diesen Daten können die Parteien mit ausgewählten politischen Inhalten bestimmte Wechselwählergruppen gezielt ansprechen. Den meisten ist ja gar nicht bekannt, dass

seit langem die Werbung auf den Internetseiten, die sie aufsuchen, «personalisiert», d.h. aufgrund des Profils der Nutzer maßgeschneidert auf ihre wahrscheinlichen (erwarteten) Bedürfnisse zugeschnitten ist. «Nutzer, die diese Seite aufsuchten, interessierten sich auch für diese Inhalte», heißt es zum Beispiel bei Amazon.

Die Wissenschaftler schließen aus ihrer Studie, dass es sehr einfach ist, Teilnehmer sozialer Netzwerke (Facebook ist das am meisten verbreitete, eigentlich ein No-Go...) mithilfe von personalisierter Wahlwerbung zu beeinflussen, ihre Vorlieben gezielt auszunutzen. Sicher liegt zwischen Werbung und Entscheidung noch ein großer Schritt. Aber die Prognosemöglichkeiten der Maschinen über das Verhalten von Menschen werden genauer, je mehr Daten von Teilnehmern gesammelt werden. Manipulationsmöglichkeiten sind daher nicht von der Hand zu weisen für die größer werdende Gruppe von Menschen, die ? mit dem allgegenwärtigen Smartphone in der Hand ? ihre Informationen fast nur aus dem Netz beziehen und damit Mikro- oder Nanotargeting ausgesetzt sind.

Inzwischen gibt es mehrere Wissenschaftler und Organisationen (Chaos Computer Club, netzpolitik.org usw.), die in Sorge um die unkontrollierte Entwicklung solcher Algorithmen eine politisch-gesellschaftliche Kontrolle fordern. Das wird sicher ein nicht leichter Streit gegen die Interessen der großen IT-Konzerne und staatlichen Organe.

Quelle: Informatik Spektrum, August 2017