Alles offen

Wieviel Freiheit bringt uns die totale Technologie?

→ *von Christoph Pfluger*

Das Internet hat uns die grosse Befreiung versprochen: Alle können fast alles wissen und sich mit jedem verbinden, um gemeinsame Träume zu verwirklichen. Aber wirklich alles wissen, das können nur die grossen Geheimdienste und die noch viel grösseren privaten Datensammler mit ihren riesigen Rechenzentren. Sie haben die grosse Freiheit, uns zu kontrollieren und zu beeinflussen; uns bleibt die Aufgabe, damit irgendwie zurechtzukommen. Wie das geht, erklärte Google-Chef Eric Schmidt schon 2009: «Wenn es etwas gibt, von dem du nicht willst, dass es jedermann weiss, dann solltest du es vielleicht gar nicht tun.» Aha: Wir sollen also nur noch tun, was Normen entspricht und kein Aufsehen erregt. Ein nicht legitimiertes Konglomerat von privaten und staatlichen Datenkraken bestimmt also das Bild des Menschen – das faschistische Ideal einer Gesellschaft.

Ein andere Begründung, den Verlust der Privatsphäre hinzunehmen, ist «wahre Authentizität», ein Begriff, den die Facebook-Managerin Sheryl Sandberg verwendet. Die private Person, die wir sind, soll mit der gesellschaftlichen Person eins werden. Oft zu hören ist auch der Satz «ich habe nichts zu verbergen». Wer mit einer solchen Aussage ernst genommen werden will, soll bitte zuerst eigene Sex-Videos und die Steuererklärung ins Netz stellen.

Das Verschwinden der Privatsphäre ist erst der Anfang; jetzt kommt der Kontrollverlust über unser Leben. Treiber sind ausgerechnet die kleinen intelligenten Helfer, die uns das Leben erleichtern sollen und über das Internet of Things (IoT) miteinander verbunden sind: intelligente Thermostate, Lichtschalter, Kühlschränke, Babyphones etc., alles smart – und leicht zu hacken. Denn die Sicherheitsstandards für die kleinen Dinger liegen weit hinter denen zurück, die für Personal Computer gelten, und die sie schon ungenügend. Als ein Drucker des Department of Commerce in Washington letzthin ein Dokument in chinesischer Sprache ausdruckte, führte eine Untersuchung des FBI zur Erkenntnis, dass die Chinesen über ein smartes Thermometer in das Computersystem der Behörde eingedrungen waren und sich dadurch optimal auf die Verhandlungen vorbereiten konnten – bis jemand in Peking offenbar einen falschen Druckbefehl auf die Reise schickte. Der grösste Diebstahl von Finanzdaten, den Transaktionen von 110 Millionen Kunden des US-Detailhändlers «Target», begann ebenfalls ganz harmlos: bei einem Mitarbeiter der externen Hauswartungsfirma. Der Mann lud sich unwissentlich einen Trojaner auf seinen Rechner. Von dort fand er seinen Weg in das Heizungssystem von Target, dann in das Hauptnetzwerk und schliesslich an die Kassen, wo etliche Monate lang alle Zahlungsdaten von den Hackern gesammelt wurden.

Wir tun so, als ob wir uns mit einer Sonnenbrille vor einer nuklearen Kernschmelze schützen könnten.

Computerkriminalität ist ein riesiges schwarzes Loch, in das jeder fallen kann, der ein Handy, einen Computer oder irgendein smartes Ding besitzt. Der für Interpol in 70 Ländern tätige Internetkriminalist Marc Goodman hat dazu ein phantastisches Buch geschrieben, in dem er auf 500 Seiten ungefähr jede Illusion zerstört, die man zum Internet haben kann («Future Crimes», Anchor Books, 2015. Auf deutsch: «Global Hack», Hanser, 2015)

Jeder kann sich heute im Darknet für 500 bis 2000 Dollar komplette Softwarepakete zum Datenklau kaufen. Vieles läuft auch ganz legal: Die Gelegenheit, alle mobilen Daten zu besitzen, war der Grund, warum Google sein Android-Betriebssystem für Mobiltelefone kreierte und es gratis an Entwickler und Anwender verschenkte, schreibt Goodman. 82 Prozent der Android-Apps verfolgen die online-Aktivitäten ihrer Nutzer und erstaunliche 80 Prozent sammeln Angaben über den Aufenthaltsort, auch so scheinbar harmlose Spiele wie das weit verbreitete «Angry Birds». Warum wohl kaufte Google 2014 den kleinen Hersteller von intelligenten Thermostaten «Nest» für exorbitante 3,2 Mrd. Dollar? Ihre Geräte verfügen über Bewegungsmelder und wissen, wann jemand zuhause oder in den Ferien ist – und sie können selbstverständlich gehackt werden.

Die ganz grossen Gefahren liegen aber noch vor uns: in der Analyse unseres Verhaltens (zum Beispiel aufgrund unseres Tipp-Rhythmus' auf der Tastatur), der kompletten Digitalisierung unseres individuellen Genoms (gewisse Firmen verlangen von ihren Mitarbeitern bereits eine DNA-Analyse) oder der Digitalisierung und Synthetisierung der Biologie. Der enormen Risiken einer Cyber-Attacke auf die digitalisierte Welt oder ihren Missbrauch sind wir weitgehend unbewusst. Wir tun so, schreibt der bekannte Statistiker Nate Silver, als ob wir uns mit einer Sonnenbrille vor einer nuklearen Kernschmelze schützen könnten.

Was tun? Marc Goodman tönt auch am Schluss seines Buches nicht wirklich optimistisch: «Wir haben nicht nur ein IT-Problem. Weil die Technologie mit unserem modernen Leben vollkommen verwoben ist, haben wir auch ein gesellschaftliches Problem, ein persönliches Problem, ein Finanzproblem, ein Gesundheitsproblem, ein Produktionsproblem, ein Sicherheitsproblem, ein Regierungsproblem, ein Transportproblem, ein Energieproblem, ein Privatheitsproblem, und ein Menschenrechtsproblem. Wir haben keine andere Wahl, als diesen Kampf zu gewinnen, … weil die Alternative zu schrecklich ist, um daran zu denken. Dies muss ein Aufruf zum Handeln sein.»
Jetzt haben wir diesen Aufruf mindestens gehört. Das Ergebnis ist offen.