Handelsblatt
RESEARCH INSTITUTE
ANALYSE

Digitalisierung – 6. März 2020

Mündig statt bequem

Greift der Trend zur totalen digitalen Überwachung von Asien nach Europa über? Es liegt an uns, die Vorteile des Internets zu nutzen und die Nachteile auszuschalten.

von Prof. Renate Schubert

Überwachungskameras stehen in Singapur an jeder Ecke, öffentliche Sicherheit wird groß- und der Schutz der Privatsphäre kleingeschrieben. Da passt der neue Coup des Stadtstaats ins Bild: die digitale Gesichtserkennung bei Abgeordneten. Wollen die Politiker das Parlament betreten, müssen sie nicht mehr ihre Zugangsberechtigung zeigen, sondern sich einer „facial recognition“ unterziehen. Im Lichte der vergangenen Jahre wäre es keine Überraschung, wenn die überschaubare Zahl der Abgeordneten künftig als Vorzeigeprojekt für die Gesichtserkennung in Menschenmengen diente.

Damit würde sich Singapur auf den Weg Chinas begeben. Die Volksrepublik ist gerade dabei, das öffentliche und private Leben flächendeckend zu kontrollieren und einen totalen digitalen Überwachungsstaat zu etablieren. Gesichtserkennung spielt hier eine ebenso große Rolle wie das Sozialpunktesystem, das jedes abweichende Verhalten sanktioniert. Individuelle Rechte haben in China derzeit wenig Chancen. Orwell lässt grüßen.

Erfasst der Trend bald auch Europa? Immerhin gab es ja schon Pilotprojekte zur individuellen Gesichtserkennung in anonymen Massen, beispielsweise am Bahnhof Südkreuz in Berlin. Und auch Flughäfen setzen auf digitale Kontrollen, bei denen das Gesicht fotografiert und mit dem Passfoto abgeglichen wird. Dabei geht es aber, anders als in China, nur um einfache Verifikationen, nicht um den Abgleich mit einem vollständigen Datenportfolio. Digitale Verfahren, bei denen mithilfe von Fotos die namentliche Identität einer Person festgestellt wird, sind ungleich komplexer und erfordern den Vergleich von Tausenden von Bildern. So schnell wie in Asien wird die flächendeckende Gesichtserkennung in Europa wohl kaum Einzug halten.

Unbestreitbar ist allerdings, dass auch in Europa staatliche Stellen und private Firmen über unzählige Daten verfügen – Daten, die wir in der Regel durch unser digitales Verhalten selbst „produzieren“. Müssen wir uns deshalb Sorgen machen? Oder profitieren wir eher vom ständigen Datensammeln?

Eine eindeutige Antwort gibt es nicht. Denn die Nutzung der Datenströme bringt Vorteile, beeinträchtigt aber auch unsere Privatsphäre. Verzichten wir auf die Datenauswertung, ist das gut für die Privatsphäre, aber schlecht für treffsichere staatliche und privatwirtschaftliche Angebote, die unseren Präferenzen entsprechen.

Zu den Vorteilen der Datenstrom-Analyse gehört zweifellos, dass Staat und Unternehmen die Wünsche und Abneigungen ihrer Klientel gut kennen und ihre Angebote mithin zielgerichtet auf deren Vorlieben ausrichten können. Sind wir aber zum Beispiel auch bereit, eine Preisdiskriminierung hinzunehmen, bei der jene Käufer, die ein bestimmtes Produkt immer wieder haben wollen, dafür einen höheren Preis zahlen müssen als solche, die es nur ab und zu kaufen?

Derartige Preisdiskriminierungen, mit denen die Zahlungsbereitschaft der Nachfrage optimal abgeschöpft werden soll, kennen wir zwar schon aus den Ökonomie-Lehrbüchern. Die moderne, digitale Preisdiskriminierung unterscheidet sich von der klassischen aber dadurch, dass sie „verdeckt“ stattfindet und nicht offen. Genau darin liegt das Problem. Eine Schweizer Handelskette musste den Versuch, eine digitale Preisdiskriminierung einzuführen, nach der „Enttarnung“ jedenfalls sofort abbrechen – zu laut war der Aufschrei.

Bei transparenter Kommunikation bietet die Datenanalyse durchaus Vorteile, beispielsweise auch mit Blick auf unsere Mobilität. So können dank der Tracking-Funktionen unserer Smartphones die Verkehrsflüsse in Städten relativ genau verfolgt und prognostiziert werden. Einen entsprechenden Datenzugang vorausgesetzt, erhalten die Kommunen Material für eine bessere Verkehrsplanung und einen sinnvolleren Infrastrukturausbau. Sie erfahren beispielsweise, wo Straßen ausgebaut oder verstärkt Fahrradwege angelegt werden sollten.

Interessanterweise besteht das Geschäftsmodell vieler Handy-basierter Fahrrad-Vermietungsfirmen heute im Kern nicht mehr darin, Fahrräder zu vermieten, sondern Verkehrsflussdaten an Städte und Gemeinden weiterzuverkaufen. Die Kehrseite der digitalen Medaille: Als einzelne Person weiß man meist nicht, wer die Mobilitätsdaten eigentlich besitzt und wer welche Auswertungen und Abgleiche mit anderen Datenbanken vornimmt.

Das verunsichert und weckt Zweifel. Deshalb kommen nicht wenige auf die Idee, die Weitergabe ihrer Daten zu unterbinden. Bei nüchterner Abwägung der Vor- und Nachteile – komfortable Nutzung der Miet-App versus erheblicher Aufwand, das Fahrrad an einer bestimmten Station abzuholen und später dort auch abgeben zu müssen – tritt der Datenschutzimpuls dann häufig doch wieder in den Hintergrund.

Aus gesellschaftlicher Perspektive ist das sogar positiv, denn je weniger Mobilitätsdaten vorhanden sind, desto schwieriger wird die künftige Verkehrsplanung. Die Gesellschaft profitiert an dieser

Stelle von einem Phänomen, das unter dem Begriff „Privacy Paradox“ bekannt ist: Wir alle geben an besorgt zu sein, dass Unbefugte an unsere privaten Daten kommen. Gleichzeitig unternehmen die meisten aber fast nichts, um ihre privaten Daten effektiv zu schützen. In dieser Hinsicht sind wir alle allzu bequem. Entsprechende Einstellungen auf den elektronischen Geräten werden selten aktiviert – zum Teil, weil man sie gar nicht genau kennt, zum Teil aber einfach auch, weil es zu umständlich erscheint.

Was bedeutet das nun? Die Analyse der Datenströme kann vorteilhaft für Staat, Unternehmen und Bürger sein. Dies gilt umso mehr, je weniger die Bürger Grund zum Unbehagen haben. Staat und Wirtschaft sollten also klar kommunizieren, welche Daten sie wie nutzen beziehungsweise an wen weitergeben. Das Einhalten komplizierter und teilweise schwer verständlicher Datenschutz-Richtlinien reicht nicht. Gefragt sind verständliche Informationen – und einfache Möglichkeiten für ein Opt-Out aus der Datenakkumulation. Notwendig ist auch ein „Empowerment“ der Bevölkerung, das den Grad an Autonomie und Selbstbestimmung im digitalen Zeitalter erhöht.

Denn nur wer versteht, was von wem aus dem Datenstrom gefischt wird und mit welchen Konsequenzen diese Fischzüge verbunden sind, kann eigenverantwortlich entscheiden, welche Daten freigegeben und welche Firmen für vertrauenswürdig gehalten werden. Statt bequem sollten wir uns digital mündig verhalten, um den Vorteil der Daten hoch und die Nachteile tief zu halten.