Was wir von uns preisgeben…

Verbraucher und ihre Verantwortung

Hans-Georg Eberhard

Hans-Georg Eberhard

■ Jeder Klick im Internet hinterlässt Spuren. Tausche Daten gegen Dienste – dies ist das Geschäftsprinzip von Google, Facebook und Co. Die jüngste Facebook-Enthüllung zeigt einmal wieder, das: Daten der Nutzer missbraucht werden. Die Quelle der gesammelten Daten ist der Nutzer selbst, Facebook ist kein Einzelbeispiel. Ich schaue mir ein beliebiges Smartphone an: Vier Apps dürfen den Standort abrufen: Google Maps, WhatsApp, Chrome und »Fotos«, die Fotogalerie. Sechs Apps dürfen die Kontakte im Telefonbuch einsehen. Zwei Apps können erkennen, ob gerade telefoniert wird und wenn ja, mit wem. Sieben Apps können die »WLAN-Verbindungen« abrufen und damit immer, wenn das WLAN eingeschaltet ist, erkennen, wo sich das Smartphone befindet. Der Nutzer als unfreiwilliger Datenlieferant. So werden wir User zum Datenlieferanten, im Kleingedruckten stimmen wir der Nutzung und Weitergabe der Daten zu, den Umfang und die Bedeutung dieser Zustimmung kann der User kaum überblicken.

Einige Beispiele:

Die meistgenutzte Suchmaschine Google wertet den Verlauf des Browsers, Suchanfragen, die Standorte des Android-Smartphones und Gmail-Nachrichten aus. Google Search History speichert detailliert, was über Google gesucht wurde. Google Preferences analysiert jeden Schritt im Netz und erstellt daraus ein Grundprofil, das etwa Informationen zum Geschlecht, Alter und den eigenen Interessen beinhaltet. Google Location History ermittelt bei Android-Geräten ständig den Standort, sofern diese Funktion nicht deaktiviert wurde. WhatsApp sammelt trotz Verschlüsselung die Meta-Daten der Benutzer. Verschlüsselt wird mittlerweile, was mitgeteilt wird – wer, wann und mit wem kommuniziert, das weiß WhatsApp trotz Verschlüsselung weiterhin. Beim Telefonieren über WhatsApp werden die Telefonnummern, der Zeitpunkt des Anrufs, die Anrufdauer gespeichert. In der Spielekonsole Xbox eingebaute Kameras und Hochfrequenzmikrofone senden Ton und Bilder auf die Datenserver von Microsoft. Aus diesen Daten lassen sich u.a. Reaktionsgeschwindigkeit und die Lernfähigkeit des Spielers ermitteln, daraus werden Rückschlüsse auf die emotionalen Zustände der Spieler gezogen. Der intelligenter Rauchmelder »Nest«, ein Produkt des Google Konzerns, erkennt unter anderem, wie viele Personen sich wie lange in welchen Zimmern aufhalten – und schickt diese Daten an Google. Diese Liste lässt sich fortführen. Entscheidend ist nicht, an wen wir noch Daten liefern, sondern was mit damit geschieht.

Was mit unseren Daten passiert

Gegen eine zielgerichtete, auf den Nutzer abgestimmte Werbung ließe sich kaum etwas sagen. Politik und Konzerne entwickeln schon längst Modelle, um die Daten in einem weitaus größeren Umfang zu nutzen, als wir es uns heute vorstellen können.

Social-Media-Profiling ist »die Berechnung der Kreditwürdigkeit einer Person mit den Daten, die im Internet verfügbar sind«, so Michael Maifarth von PricewaterhouseCoopers International Deutschland. Datenbasis sind die Social Media-Profile potentieller Kreditnehmer: Facebook, Xing, Twitter. Was in den Profilen der User auf öffentlich gestellt ist, darf jeder einsehen und verwenden. Beim sogenannten »Opt-In«-Verfahren geben die Kreditnehmer der Bank die Erlaubnis, auch die nicht-öffentlichen Teile ihres Profils einzusehen. Aus den so gewonnen und gesammelten Daten werden Wahrscheinlichkeiten gebildet. Die Wahrscheinlichkeit, dass ich einen Kredit zurückzahlen werde, ist höher, wenn ich auf meinen Facebook-Fotos einen Anzug trage und nicht betrunken bin. Oder wenn ich viele Freunde habe, die Geld haben. Oder wenn ich häufiger in die Oper oder ins Theater gehe. Die Algorithmen des Scorings und die Datenbasis für das Scoring und somit die individuelle Beurteilung des einzelnen werden nicht offengelegt.

Wer wird kriminell?

In Chicago sammelt die Polizei öffentlich zugängliche Daten und erstellt damit einen Gefährlichkeitswert; einen Wert, der aussagen soll, wie hoch die Wahrscheinlichkeit ist, dass der Betroffene in naher Zukunft in ein Verbrechen verwickelt sein wird. Verwickelt meint hier: »zum Täter wird«. Zum Beginn des »predictive Policing« genannten Verfahrens umfasste die Liste der computerberechneten gefährlichsten Leute 350 Menschen, mittlerweile sind es 4000. Es gibt keine Möglichkeiten, von der Liste wieder herunterzukommen. Die Unschuldsvermutung wird de facto ausgehebelt. Die deutsche Variante des »predictive Policing« ist die Analysesoftware »PreCob«. Es geht »nur darum, mit mathematischen Formeln zu berechnen, an welchem Ort und zu welchem Zeitpunkt wahrscheinlich der nächste Einbruch stattfinden wird.

China – Die maschinenlesbare Bevölkerung

In der Volksrepublik China soll ab 2020 soll ein »Social Credit System« für alle Bürger verpflichtend werden. Geplant sind Bonuspunkte für staatstreues Verhalten, Abzüge für Regimekritik. Die Dating-App B aihe greift auf den Punktwert seiner Mitglieder zu. Wer sich also nicht systemkonform verhält oder gar auf das Punktesystem verzichtet, hat schlechtere Chancen, einen Partner zu finden. Der eigene Punktewert bei Sesame Credit hängt auch von dem Punktewert der Freunde ab. So werden Menschen isoliert, die nicht dem Punkteschema entsprechen. Dennoch wird das System von der Bevölkerung überaus positiv gesehen – die Dienste werden als sinnvolle Ergänzung der Online-Dienste verstanden.