Social Scoring ist das nächste große Geschäft der Datenkraken. Frei im Internet verfügbare Informationen aus sozialen Netzwerken oder anderen Quellen werden von Algorithmen verknüpft und zu einem Wert zusammengemischt. In totalitären Regimen wie China wird Social Scoring im großen Maßstab eingeführt. Wem Reste seiner Privatsphäre wichtig sind, sollte wissen, worum es geht – und wieso es nicht egal ist, was man online macht

Beliebige Zahlen statt Menschen? Social Scoring möchte aus Individuen in letzter Konsequenz gläserne Datenmodelle machen. FOTO: ADOBE STOCK

Die wissen wollen, was wir tun werden

VON STEPHAN ZENKE

REUTLINGEN. Social Scoring ist so gefährlich wie das Ozonloch. Nichts zu sehen, nichts zu riechen, nichts zu hören – aber die Auswirkungen sind verheerend. Der Mensch wird mit allen über ihn in der digitalisierten Welt verfügbaren Daten eingeordnet und bewertet, sein zukünftiges Verhalten vorhergesagt. Was das bedeutet, lässt sich schon heute in China beobachten. Es lohnt sich, genau hinzuschauen.

Das in China geplante staatliche »Sozial-Kredit-System« soll nicht nur die Kreditwürdigkeit jedes Bürgers bewerten, sondern ebenfalls viele weitere Aspekte des Verhaltens. Wer häufig bei Rot über die Ampel geht, zu lange an seinem Smartphone spielt, ungesunde Lebensmittel kauft oder nach regimekritischen Seiten im Internet sucht, wird mit einem niedrigen Scorewert bestraft. Dann dürfen etwa seine Kinder nicht mehr in bessere Schulen gehen, kann er seine berufliche Karriere vergessen und so weiter und so fort. All das scheint weit weg, ist aber dennoch ein Problem für uns. Weil Verfahren des Social Scoring auch hierzulande wirtschaftlich verlockend erscheinen. Wer das Prinzip verstanden hat, ist einen Schritt weiter.

Je mehr Daten, desto besser

»Social Scoring bedeutet, möglichst viel aus möglichst vielen Bereichen über eine Person zu erfahren. Je mehr Daten, umso besser«, beschreibt der baden-württembergische Landesbeauftragte für den Datenschutz, Dr. Stefan Brink, das Verfahren. Um sich vorzustellen, was den Datensammlern schmeckt, reicht ein Blick auf die Mehrheit der Android-Smartphones. In den Standardeinstellungen kriegen Google und Co. mit, was mit dem Gerät gemacht wird: wie oft wir was nutzen, wonach wir suchen, wo wir uns bewegen. Populäre Apps wie Facebook oder WhatsApp sammeln ebenfalls Daten, um nur zwei weitere Beispiele zu nennen. Doch niemand weiß so genau, was da eigentlich über ihn zusammengetragen wird und wer sich wie daraus eine Bewertung zusammenbastelt. »Die Intransparenz bei Social Scoring beruht darauf, dass in der Fülle der Daten der Blick darauf verloren geht, was eigentlich gesammelt wird«, sagt Brink. Jenseits dessen ist schon die Denkweise hinter dem Social Scoring erschreckend.

Keine Geheimnisse mehr

»Menschen werden nicht mehr als Individuen betrachtet, sondern als Daten-Double. Eine Konstruktion, die einen Menschen in die Summe seiner Daten auflöst«, erklärt Dr. Jessica Heesen als Leiterin des Forschungsschwerpunkts Medien- und Informationsethik an der Universität Tübingen. Ihr Kollege Dr. Thilo Hagendorff ergänzt: »Man geht davon aus, dass Daten Wirklichkeit abbilden, das ist aber nicht so«. Auch Datenschützer Brink hat eine klare Meinung: »Ich finde, Social Scoring beruht auf einer ganz grundlegenden Fehlentscheidung, und deswegen halte ich nichts davon. Nämlich auf der Idee, man könnte Menschen umfassend erfassen. Man könnte ihre Persönlichkeit so komplett abbilden, dass der Mensch wie ein offenes Buch ist, dass der Mensch keine Geheimnisse mehr hat, er vollständig wirtschaftlich verwertbar und dann möglicherweise auch politisch steuerbar ist. Das ist schon vom Grundgedanken her ein offensichtlicher Verstoß gegen das Menschenbild, das uns mitgegeben ist, das unserer Verfassung, die die Würde des Menschen schützt.« Nur wenige Beispiele machen deutlich, wie schnell jeder in einen völlig falschen Topf geworfen werden könnte.

Wer den Suchbegriff »Hitler« eingibt, könnte ein Neonazi sein oder aber genau das Gegenteil. Wenn auf seinem Rechner viele Computerspiele für Datenverkehr sorgen, mag das ein Hinweis auf Suchtverhalten sein, möglicherweise stecken dahinter aber eher seine Kinder. Der Wohnort mit vielen säumigen Schuldnern in der Nachbarschaft sagt eigentlich gar nichts über die Kreditwürdigkeit aus. »Es können falsche Zuordnungen entstehen. Wir werden nicht entsprechend unserer Person und Leistung beurteilt«, macht die Tübinger Medienethikerin Dr. Jessica Heesen deutlich. Müssen wir uns in Deutschland vor einem »Sozial-Kredit-System« wie in China fürchten?

Wer die Datenkraken sind

»Technisch denkbar wäre das, aber rechtlich komplett ausgeschlossen. Das ist so offensichtlich rücksichtslos und bürgerrechtsfeindlich, was da in China passiert. Das ist ein abschreckendes Beispiel«, gibt Landesdatenschützer Dr. Stefan Brink Entwarnung. Der Rechtsstaat sei eben keine Datenkrake, er dürfe nur dann Daten sammeln und auswerten, wenn er dazu eine gesetzliche Grundlage hat. Der Staat sammelt immer gezielt. Das unterscheidet ihn von wirtschaftlich getriebenen Datensammlern, die einfach mal alles probieren.

Die Jäger und Sammler der digitalen Neuzeit sind meist amerikanische Konzerne, die ihre Fährten fast überall im Internet ausgelegt haben. »Das Problem ist, das Strukturen wie Google monopolartig sind«, meint Jessica Heesen. »Im Durchschnitt geben neun von zehn Webseiten Nutzerdaten an Dritte weiter«, beschreibt Thilo Hagendorff die unsichtbaren Formen der Datensammelei. Verfahren des Social Scoring sind längst ein Thema in der Privatwirtschaft. »Na klar, wir sind in einem Übergang, und wir müssen versuchen das Ganze so zu steuern, dass es sich in einem erträglichen Rahmen bewegt«, betont Datenschützer Brink. Eine GEA-Anfrage bei lokalen Banken und der Versicherungswirtschaft ergibt recht kurze Antworten.

So sagt etwa Andreas Lehmann als Pressesprecher der Kreissparkasse Reutlingen: »Social Scoring im Kontext einer Überwachung von Bürgern (oder in unserem Fall Kunden), wie derzeit häufiger aus China berichtet wird, gibt es bei der Kreissparkasse nicht.« Eine Sprecherin der Commerzbank in Stuttgart, die ihren Namen nicht in der Zeitung lesen möchte, betont: »Social Scoring wird in der Commerzbank nicht eingesetzt und es gibt derzeit auch keine Pläne für den Einsatz eines solchen Verfahrens.« Christian Ponzel vom Gesamtverband der Deutschen Versicherungswirtschaft gibt lediglich zu Protokoll, »wir wissen, dass Unternehmen in bestimmten Fällen Scorewerte bei (unterschiedlichen) Auskunfteien abfragen, um die Bonität eines Kunden beurteilen zu können«. Klar ist laut einer repräsentativen Bevölkerungsbefragung der Beratungsgesellschaft Pricewaterhouse-Coopers vom Mai 2018 mit dem Titel »Ist Deutschland bereit für Social Scoring?« eines: Verbraucher nehmen Social Scoring als Risiko wahr. (GEA)

WAS SOCIAL SCORING IST

Kaum eine andere allgemein zugängliche Quelle bietet so viele Informationen über eine Person wie die sozialen Netzwerke. Einige Unternehmen arbeiten bereits mit dem Geschäftsmodell der systematischen Auswertung von Daten aus sozialen Netzwerken, dem sogenannten Social Scoring.

Aber nicht nur »die falschen« Freunde oder Posts bei Facebook, Xing oder Twitter können sich negativ auf Bonitätsprognosen auswirken. Auch die technischen Eigenschaften des Geräts, von dem aus eine Kreditanfrage gestartet wurde, die Uhrzeit, zu der eine Bestellung abgegeben wurde oder öffentlich zugängliche Informationsquellen wie das Bewertungsprofil bei Ebay können unter Umständen in automatisierte Bonitätsbeurteilungen einfließen. Solchen Praktiken strenge gesetzliche Grenzen zu setzen und für eine effektive Durchsetzung der Vorschriften zu sorgen, wird deshalb in den kommenden Jahren eine der zentralen Herausforderungen für die Daten- und Verbraucherschutzpolitik auf Bundes- und EU-Ebene sein.

Wer also viel und aktiv im Internet – speziell in sozialen Netzwerken – unterwegs ist, muss sich stets der Tatsache bewusst sein, dass er bei allem, was er tut, eine Datenspur hinterlässt. Und weil viele Verbraucherinnen und Verbraucher in der heutigen Zeit nicht gänzlich auf solche Aktivitäten verzichten können oder möchten, heißt die Devise Datensparsamkeit! (Quelle: Verbraucherportal Baden-Württemberg)

WAS JEDER TUN KANN

Es ist eben nicht egal, was man im Internet tut oder lässt. Digitaler Selbstschutz gegen Social Scoring bedeutet zunächst mal ein grundlegendes Bewusstsein zu entwickeln: Alles, was man im Internet macht, kann ohne Gegenmaßnahmen erfasst werden. Alles, was man an Daten im Internet hinterlässt, kann von Dritten ausgewertet werden. Daher ist der erste Schritt zu mehr Sicherheit simple Datensparsamkeit. Muss man wirklich in allen sogenannten sozialen Netzwerken mitmachen? Und falls ja, muss man wirklich den ganzen Tag angemeldet bleiben, und auch noch die dazugehörige App auf dem Smartphone nutzen? Beispiel: Wer Facebook ohne sich abzumelden auf Computer und Smartphone gleichzeitig nutzt, und dann auch noch WhatsApp verwendet, der hinterlässt eine fette Datenspur. Ist es wirklich notwendig, seinen gesamten Konsum in diverse internette Kaufhäuser zu verlagern? Bei jedem Online-Shoppingbummel entsteht ein Berg von Informationen von der Suche nach dem passenden Artikel bis zur Wahl der Zahlungsart. Wer offline kauft und bar bezahlt, hinterlässt kaum Spuren. Kein riesiger Aufwand ist es auch, den Webbrowser – ganz egal welchen – im privaten oder Inkognito-Modus zu verwenden, und regelmäßig den Verlauf komplett zu leeren, weil dadurch das Tracking erschwert wird. Doch dies sind alles nur Beispiele. Verweise auf noch viel mehr praktische Tipps zur digitalen Selbstverteidigung gibt's in der Infobox. (zen)

DIGITALE SELBSTVERTEIDIGUNG

Zum Nachlesen und Nachschauen

Wissen ist gerade dann Macht, wenn es um den Schutz der eigenen Daten geht. Netterweise gibt's online jede Menge Quellen: Eine Fundgrube für alle politisch Interessierten, denen ihre Daten lieb und teuer sind, ist www.netzpolitik.org. Hier gibt's viel zum Thema Social Scoring.

Die Digitale Gesellschaft der Schweiz hat einen Ratgeber »Anleitung zur digitalen Selbstverteidigung« veröffentlicht: www.digitale-gesellschaft.ch und oben rechts die Suche nutzen.

Mythen und Fakten zu Überwachung und digitaler Selbstverteidigung hat die Rosa Luxemburg Stiftung in einer Publikation mit dem Titel »Offenes Geheimnis« gesammelt: www.rosalux.de und auch hier den Suchbegriff eingeben.

Der Verein Digitalcourage informiert auf seiner Website unter Projekte über »Digitale Selbstverteidigung«: digitalcourage.de ganz unten auf der Startseite. Wer sich kritisch mit den Themen »IT-Sicherheit« und »Datenschutz« befassen möchte, wird sich den Kuketz-Blog gerne merken: www.kuketz-blog.de

Das Bundesamt für Sicherheit in der Informationstechnologie bietet ein verständliches Angebot zum Thema inklusive aktuellen Hinweisen auf Sicherheitslücken in Software und Gegenmaßnahmen sowie einer kostenlosen Hotline: www.bsi-fuer-buerger.de (zen)