KAPITALISMUSKRITIK 23.04.2018 | Jennifer Cobbe

Überwachungskapitalismus

Im Internet hat sich ein Geschäft mit unseren Daten durchgesetzt. Das sollten wir beenden.

Lesen Sie diesen Beitrag auch auf Englisch.

Erfunden von Google und mittlerweile von den meisten Internet-Dienstleistern – Facebook, Amazon, LinkedIn und anderen – in der einen oder anderen Form genutzt, generiert ein Modell umfassender Überwachung und der Beeinflussung des menschlichen Verhaltens Gewinn: der Überwachungskapitalismus. Die mit dieser Maschinerie gesammelten Daten ermöglichen auch das Mikrotargeting durch politische Organisationen und feindliche Staaten. Und der Selbstgefälligkeit ihrer Verfechter ist es zu verdanken, dass sich Desinformation und Extremismus ausbreiten können.

Die beteiligten Unternehmen folgen unseren Spuren im Internet und im Alltag, beobachten und speichern möglichst viel von dem, was wir tun. Durch den Verzicht auf Datenschutz lassen wir es zu, dass die Unternehmen von jedem von uns ein umfassendes Datenprofil erstellen.

Diese Profile enthalten nicht nur die Informationen, die wir selbst über uns liefern, sondern auch solche, die diese Firmen aus ihrem umfassenden Wissen über unsere Interessen und unser Verhalten ableiten. Solche Schlussfolgerungen mit sensiblen und sogar scheinbar geheimen Informationen lassen sich mit unglaublicher Genauigkeit ziehen. In die Profile fließt darüber hinaus das durch ständiges Experimentieren gewonnene Wissen darüber ein, welche Werbung uns am wirkungsvollsten dazu veranlasst, bekannte Abkürzungen in der Entscheidungsfindung – der Heuristik – zu nehmen und entsprechend zu klicken. Wenn wir ins Internet gehen, nehmen wir oft unbewusst an zahlreichen Experimenten teil, mit denen eruiert werden soll, wie uns die Unternehmen das Geld leichter aus der Tasche ziehen können.

Der Zugang zu diesem Profil wird dann – gemeinsam mit den einflussreichen Tools zur Verhaltensbeeinflussung, die darauf zurückgreifen – auf dem Werbemarkt gewinnbringend verkauft. Die Internetunternehmen erstellen faktisch ein detailliertes Modell unserer

Interessen, Verhaltensweisen und psychischen Schwächen und knöpfen anschließend Werbekunden Geld dafür ab, dass sie es zu ihrem eigenen Vorteil gegen uns verwenden können.

Wenn sich Unwahrheiten ungehindert ausbreiten

Wie nicht anders zu erwarten, sind auch Wahlkampfteams sehr daran interessiert, das Verhalten von Menschen zu analysieren, Profile ihrer Interessen und ihres Handelns zu erstellen und sie mit präzise platzierter und empirisch erprobter Werbung anzusprechen. Mit Facebook-Tools wie Custom Audiences und Lookalike Audiences können politische Gruppierungen Wählerinnen und Wähler in großer Zahl erreichen. Und da diese Werbung personalisiert ist, erhalten keine zwei Wähler dieselbe Wahlwerbung. Am Tag des dritten Fernsehduells vor der US-Präsidentschaftswahl 2016 schickte beispielsweise Donald Trumps Wahlkampfteam seine Werbung in 175 000 Variationen los und sprach damit Wählerinnen und Wähler zielgerichtet an.

So entfernen sich Politik und Wahlkampf vom öffentlichen Raum, in dem Ideen überprüft, Widersprüche aufgedeckt und falsche Behauptungen korrigiert werden können. Stattdessen spielen sich Wahlkämpfe im eher privaten Umfeld ab, wo unterschiedliche Gruppen ungehindert mit widersprüchlichen Argumenten angesprochen und Desinformation und glatte Lügen frei verbreitet werden können. Dank der mangelnden Kontrolle durch Facebook konnten in der Vergangenheit darüber hinaus auch ausländische Staaten mit Desinformations- und Manipulationskampagnen demokratische Wahlen beeinflussen.

In den US-Zwischenwahlen des Jahres 2010 führte Facebook eine eigene Untersuchung über die Wirkung politischer Botschaften auf seiner Plattform durch. Wie man feststellte, ließ sich die Wahrscheinlichkeit, dass ein Nutzer wählen ging, mit einer einzigen intelligent konstruierten Anzeige um 0,4 Prozent steigern. Das ist zunächst eine kleine Wirkung, die aber US-weit einer großen Zahl von Menschen entspricht. Schätzungen von Facebook zufolge gelang es 2010, die Zahl der Wählerinnen und Wähler um 340 000 zu erhöhen. Mikrotargeting hat also durchaus das Potenzial, in engen Wahlen und Volksabstimmungen viel bewirken.

Der Überwachungskapitalismus hat noch eine weitere negative Auswirkung auf den öffentlichen Raum. Über das „Fake News“-Problem

bei Facebook wird mittlerweile ausgiebig diskutiert, und die Ursachen liegen im Grunde auf der Hand. Wenn eine Firma ihr Geld mit Werbung verdient und es nur darum geht, Menschen an sich zu binden, sind Wahrheit, Fairness, Moral und sogar Vernunft bestenfalls zweitrangig. Facebook hatte daher kaum etwas zu gewinnen, wenn es gegen verdrehte Fakten und Extremismus vorging. Das änderte sich erst mit dem öffentlichen Aufschrei.

Doch das Problem mit den Fake News beschränkt sich nicht auf Facebook. Auch Google ist betroffen, wenn Desinformation und Verschwörungstheorien in Suchergebnissen, den eigenen Nachrichten und an anderen Stellen bevorzugt werden. Unmittelbar nach dem Massenmord von Las Vegas im Oktober 2017 brachte Google News beispielsweise vorrangig Berichte, in denen der Täter als „ultralinker Irrer“ beschrieben wurde, und streute auch andere politisierte Desinformationen über die Tat. Sogar auf Faktencheck-Websites platziert Google Werbung mit Falschinformationen.

YouTube, das zu Google gehört, hat Nutzer nachgewiesenermaßen wiederholt Videos angeboten, die Extremismus, Desinformation und Verschwörungstheorien verbreiten. Das Portal wurde deshalb schon als die einflussreichste Radikalisierungsmaschine des 21. Jahrhunderts bezeichnet. Sogar Amazon, das die Überwachung für seine Empfehlungen nutzt, geht in diese Richtung. Einem Bericht der britischen Channel 4 News zufolge empfahl die Website Käufern, die gezielt danach suchten, Zutaten für die Herstellung von Bomben.

Wie staatlich reguliert werden soll

Die anstehende Datenschutz-Grundverordnung (DSGVO) der EU, die den Schutz personenbezogener Daten stärkt, ist ein Schritt in die richtige Richtung. Die DSGVO, die Ende Mai eingeführt werden soll, dürfte einigen besonders schlimmen Praktiken der Überwachungsunternehmen den Riegel vorschieben und droht bei Zuwiderhandlung mit massiven Strafen. Auch die ePrivacy Regulation der Europäischen Union, die von den Überwachungsunternehmen entschieden abgelehnt wird, verspricht digitalen Datenschutz. Gemeinsam könnten diese beiden Gesetze wirklich etwas ausrichten. Die Unternehmen selbst könnten einen positiven Beitrag leisten, indem sie ihr überwachungsgestütztes Geschäftsmodell aufgeben und auf Kontext-Werbung umsteigen.

Die Einzelstaaten und die EU haben die Sache viel zu lange einfach

laufen lassen. Mit ihrer Untätigkeit haben sie das unverantwortliche Handeln der Unternehmen erst ermöglicht. Und die Angebote der Unternehmen – mit denen sie meist darauf abzielen, noch mehr Macht zu erhalten – sind im Großen und Ganzen vereinfachend und mangelhaft. Eine Regulierung, die den Überwachungsunternehmen Macht entzieht und sie zu einer sauberen Praxis verpflichtet, ist dringend notwendig.

Doch legitime Ängste vor Extremismus und Desinformation muss man sehr gut abwägen gegen das Recht auf freie Meinungsäußerung und die Notwendigkeit, auch unliebsame Ideen zu diskutieren. Auch sollten wir uns nicht der Illusion hingeben, dass künstliche Intelligenz der Übel Herr wird. Für die Bewältigung der Probleme ist mehr menschliches Eingreifen gefragt, nicht weniger. Die Automatisierung bringt nicht nur Gutes. Da also deutlich mehr getan werden muss, werden die Regierungen und die EU noch eingehend über die Problematik nachdenken müssen.

Als Gesellschaft haben wir die Probleme des Überwachungskapitalismus nun endlich erkannt. Für Veränderungen ist es nicht zu spät. Für eine gründliche Diskussion darüber, welche Rolle die betroffenen Unternehmen im öffentlichen Raum spielen und wie sie reguliert werden sollten, ist jetzt die richtige Zeit. Wir sollten die Unternehmen für ihr Fehlverhalten zur Verantwortung ziehen und Verbesserungen einfordern. Allzu lange diente das Internet vor allem Unternehmensinteressen. Doch der öffentliche Raum im Internet gehört uns allen. Es ist an der Zeit, dass wir ihn uns zurückholen.



Jennifer Cobbe
Cambridge

Jennifer Cobbe ist Forscherin am Computerlabor der University of Cambridge sowie Koordinatorin der „Cambridges`s Trustworthy Technologies Strategic Research Initiative".