Data Privacy in der Praxis

Datenschutz und Sicherheit in Daten- und KI-Projekten

DAS VORWORT

Vorwort

Angesichts der zahlreichen Vorteile der digitalen Vernetzung ist es nicht immer offensichtlich, dass futuristische Technologien auch Nachteile mit sich bringen. Instant Messaging, biometrisches Scannen, Echtzeit-Bewegungserfassung, digitaler Zahlungsverkehr und vieles mehr waren schon immer der Stoff für Science-Fiction-Fantasien. Für diejenigen unter uns, die in der Technologiebranche arbeiten (oder diese als Konsumenten erleben), ist der »Coolness-Faktor« digitaler Tools in unserer täglichen Routine schwer zu leugnen.

Die Kehrseite des digital vernetzten Lebens ist das Recht, sich vom Netz zu trennen. Für einige Tech-Millionäre der ersten Generation ist es selbstverständlich, ihre Kinder zu Hause und in der Schule vom Internet fernzuhalten. Das mag seltsam klingen, wenn man daran gewöhnt ist, die digitale Kluft als eine Trennung zwischen Besitzern von mehreren Apple-Produkten und Habenichtsen ohne 24/7-Hochgeschwindigkeitsinternet zu sehen. Da so viele unserer täglichen Interaktionen digital geworden sind, ist es jedoch für die meisten von uns eine Herausforderung, ohne unbegrenzten Onlinezugang auszukommen.

Die Nutzung digitaler Werkzeuge und der Zugang zu Onlineräumen wird uns heute genauso angepriesen wie zu Beginn des Internets: als eine bequeme, einfache Erfahrung, die völlig freiwillig ist und Spaß macht. Aber nichts ist lustig an einer Interneterfahrung, die sich wie ein Aufenthalt im Hotel California anfühlt – »du kannst auschecken, wann immer du willst, aber du kannst niemals abreisen«. Nichts ist fair an einer Onlinewelt, die das Offlineleben in Bezug auf alles einschränkt, was man sehen und tun kann und wie man behandelt werden könnte. Die Vorstellung, dass wir uns in der Internetwelt lediglich für eine Reihe von zwanglosen Interaktionen entscheiden, ist nicht mehr wahr: Wenn überhaupt, sind wir oft gezwungen, uns auf einer Autobahn zu bewegen, die mit Daten über uns und andere vollgestopft ist.

Viele von uns gehen fälschlicherweise davon aus, dass unsere Daten für alle anderen uninteressant sind. Aber in diesem Fall sehen wir nicht das ganze Bild. Moderne Apps und Algorithmen horten unsere Daten, um zu verknüpfen, wo wir leben, was wir verdienen, mit wem wir ausgehen und ob wir psychische Probleme oder eine sexuell übertragbare Infektion gehabt haben. Das passiert, wenn wir nicht erkennen, dass die Vorhersagefunktion von Algorithmen in der Regel dazu verwendet wird, ein

»Profil« von uns zu erstellen. Denn dafür werden Daten verwendet, die wir bereitwillig und unwissentlich zur Verfügung gestellt haben, wenn Anbieter uns Finanzprodukte, Versicherungsschutz, Arbeitsplätze, Wohnungen oder potenzielle Liebespartner verkaufen wollen (oder uns den Zugang dazu zu verwehren).

Digitale Konnektivität soll Spaß machen und sich nicht anfühlen, als würde man kriminell verfolgt. Aber genau dieses Gefühl war mein Einkaufserlebnis in der realen Welt, seit ich ein Kind in New York City war: Damals war es in der Regel alles andere als angenehm, als sichtbare Minderheit einkaufen zu gehen oder sich nach einem Taxi umzusehen. Ich kenne das Gefühl sehr gut, gescannt, überwacht und aus einer Gruppe herausgegriffen zu werden. Genau das zeigt ein Enthüllungsbericht nach dem anderen: Unsere privaten, persönlichen und dauerhaften Daten werden in »Profilen« zusammengefasst und an Datenhändler, Regierungen und Strafverfolgungsbehörden weitergegeben und zerstören somit unsere Privatsphäre. Genau wie bei verurteilten Kriminellen.

Der Schutz der Privatsphäre ist wie der Zugang zu einem Kredit oder einem guten Anwalt – etwas, das man besser hat und nicht braucht, als etwas, das man braucht und nicht hat. Es sollte nicht erst einer biometrischen Datenerfassung beim Einsteigen in ein Flugzeug bedürfen (wogegen ich kürzlich in San Francisco protestieren musste), um zu erkennen, dass unsere persönlichen Daten zu oft ohne unsere Einwilligung oder unser Wissen erhoben werden. Es sollte nicht nötig sein, dass eine Person, die einer ethnischen Minderheit angehört, einen datengesteuerten Gesundheits- oder Finanzalgorithmus als diskriminierend einstuft. Diejenigen von uns, die in der Technologiebranche tätig sind, sollten keine Gerichtsverfahren, Geldstrafen für Unternehmen oder staatliche Regulierung benötigen, um zu erkennen, dass Systeme, die unsere Daten fast zwangsweise abgreifen, uns weder Privatsphäre noch Wahlmöglichkeiten lassen. Und was ist mit denen, die ihre Privatsphäre bewahren wollen, indem sie offline bleiben? Ähnlich wie die Kreditwürdigkeit oder der Zugang zu einem guten Anwalt ist die Wahrung der Privatsphäre zum neuen Privileg der Wohlhabenden geworden.

Diese Kluft ist vielleicht das eklatanteste Problem unseres digital vernetzten Lebens. Wenn wir jemals zu einer digitalen Welt zurückkehren wollen, in die wir uns freiwillig begeben können, müssen wir den Raum begrenzen, in dem digitale Systeme ihre Fühler nach uns ausstrecken. Wenn wir den Menschen das Recht zurückgeben wollen, anonym zu surfen oder sich online zu melden, müssen wir die Mechanismen der Datenerfassung einschränken, die derzeit die meisten digitalen Systeme steuern. Mit *Data Privacy in der Praxis* bietet Frau Jarmul erprobte Techniken für den Aufbau einer Onlinewelt, die sich von der heutigen unterscheidet. Ihre Beispiele aus dem wirklichen Leben beweisen, dass man kein Privacy Engineer sein muss, um den Datenschutz sinnvoll zu gestalten.

Ich hoffe, dass alle, die sich über algorithmische Diskriminierung und »ethische Technologie« Sorgen machen, dieses Buch lesen werden. Darüber hinaus möchte ich jeden, der digitale Systeme entwirft, entwickelt oder testet, ermutigen, für sich selbst zu entscheiden, ob Datenschutz die Komponente darstellt, die unsere derzeitigen Onlineerfahrungen von denen unterscheidet, die wir wollen und brauchen.

– Dr. Nakeema Damali Stefflbauer
CEO, FrauenLoop and Global AI Ethics lecturer, Stanford University