GLOBAL 29.04.2019 | Magdalena Sepúlveda

Datenschutz nur für Reiche?

Weltweit wächst der Einsatz biometrischer Technologien bei der Vergabe von Sozialhilfe. Dieser Trend ist gefährlich.

Lesen Sie diesen Artikel auch auf Englisch.

In den letzten Jahrzehnten wurden die Sozialhilfeprogramme weltweit so weit ausgebaut, dass sie heute mehr als 2,5 Milliarden Menschen zugutekommen, meist den Ärmsten und Schwächsten. Der zunehmende Druck, biometrische Technologien zur Überprüfung der Identität der Versicherten einzusetzen und Informationssysteme vom Zivilregister bis hin zu Strafverfolgungsdatenbanken zu integrieren, bedeutet jedoch, dass Sozialprogramme neue Risiken für diejenigen schaffen könnten, die von ihnen abhängig sind.

Privatunternehmen, Geberagenturen und die Weltbank argumentieren, dass der Einsatz biometrischer Instrumente wie Iris- und Fingerabdruckscannen oder Gesichts- und Spracherkennung zusammen mit der Integration von Datenbanken die Effizienz steigern, Betrug bekämpfen und Kosten senken wird. Und viele Regierungen scheint das zu überzeugen. Obwohl es keine systematischen Informationen über den Einsatz biometrischer Technologien in Sozialhilfesystemen gibt, deutet ein Blick auf bestimmte Vorzeigeprogramme darauf hin, dass sie bereits im Aufwärtstrend sind.

In Südafrika erhalten 17,2 Millionen Empfänger von Sozialbeihilfen biometrische Smart Cards. In Mexiko müssen die 55,6 Millionen Versicherten von Seguro Popular (die staatliche Krankenversicherung für die ärmsten Bürger) ihre biometrischen Daten an die Behörden weitergeben. Die weltweit größte biometrische Datenbank – Aadhaar – befindet sich in Indien. Da die Aufnahme in Aadhaar eine Voraussetzung für den Zugang zu mehreren Sozialprogrammen ist, sind 95 Prozent der 1,25 Milliarden Einwohner des Landes bereits erfasst. Die Bereitstellung biometrischer Daten ist auch für den Erhalt von Leistungen in Botswana, Gabun, Kenia, Namibia, Pakistan, Paraguay und Peru erforderlich.

Der Druck, sensible Daten der Sozialversicherungen national und international zur Strafverfolgung zu nutzen, wird durch die Besorgnis über Terrorismus und Migration verstärkt.

Biometrische Daten, die in der Datenbank eines Sozialschutzprogramms gespeichert sind, können problemlos mit anderen Systemen über eine gemeinsame Kennung verknüpft werden, auch mit solchen, die nichts mit dem Sozialschutz zu tun haben, wie beispielsweise solchen für die Strafverfolgung oder das kommerzielle Marketing. In den meisten europäischen Ländern ist eine solche Datenbankintegration jedoch wegen der damit verbundenen Bedrohung für die Privatsphäre und den Datenschutz verboten. Schließlich erfordern Sozialhilfeprogramme die Verarbeitung großer Datenmengen, einschließlich sensibler Informationen wie Haushaltsvermögen, Gesundheitszustand und Behinderungen.

In vielen Entwicklungsländern, die ihre Programme zum Sozialschutz und zur biometrischen Identifizierung ausbauen, sind die Rahmenbedingungen für den Schutz personenbezogener Daten unterentwickelt. Dennoch befürworten Geber und Behörden oft eine weitestgehende Integration von Datenbanken, sowohl zwischen öffentlichen als auch privaten Einrichtungen. So verfügt beispielsweise Nigeria, das die Ausgabe von 100 Millionen biometrischen e-ID-Karten anstrebt, über eine nationale Identitätsdatenbank, die mit verschiedenen anderen Datenbanken verbunden ist, einschließlich derjenigen, die von Strafverfolgungsbehörden verwaltet werden.

Der Druck, sensible Daten der Sozialversicherungen, einschließlich biometrischer Identifikatoren, mit der Strafverfolgung – sowohl im Inland als auch international – zu teilen, wird durch die Besorgnis über Terrorismus und Migration verstärkt. Dieser Druck gefährdet nicht nur die Privatsphäre, sondern auch die bürgerlichen Freiheiten. Hinzu kommt das Risiko einer fahrlässigen Datenweitergabe oder eines unbefugten Zugriffs Dritter – auch durch Cyberkriminelle und Hacker. Sozialschutzempfänger könnten auch einer Stigmatisierung oder Erpressung ausgesetzt sein.

Außerdem besteht die Möglichkeit, dass der Zugang zu sensiblen Sozialversicherungsdaten an private Unternehmen gewährt oder verkauft wird. Sozialversicherungsbehörden und private Unternehmen wie MasterCard oder Visa schließen häufig kommerzielle Vereinbarungen ab, um Smartcards für Sozialhilfeprogramme zu entwickeln oder Unternehmen die Annahme dieser Karten zu ermöglichen. So ist

beispielsweise die biometrische Karte für Sozialhilfe in Südafrika eine MasterCard. Schlimmer noch, solche Vereinbarungen – die oft nicht öffentlich bekannt gegeben werden – enthalten in der Regel keine Rechtsbehelfe bei Daten- und Informationsmissbrauch. Jüngste Medienberichte deuten jedoch darauf hin, dass diese Risiken erheblich sind. So wurden beispielsweise in Chile Millionen von Patientenakten – einschließlich derjenigen von HIV-Patienten und Frauen, die sexuell missbraucht worden waren – fast ein Jahr lang öffentlich zugänglich gemacht.

Die Risiken, denen die Schwächsten und Benachteiligten heute ausgesetzt sind, können morgen für einen viel breiteren Querschnitt der Gesellschaft Realität werden.

Darüber hinaus nutzten private Unternehmen in Südafrika die Informationen von Millionen von Sozialhilfeempfängern, um die Unternehmensgewinne zum Nachteil der Begünstigten zu steigern. In Indien behauptete eine Zeitung, dass ihre Reporter uneingeschränkten Zugang zur Aadhaar-Datenbank erhalten hätten. Ein weiterer Bericht dokumentierte, wie Aadhaar-Zahlen mit sensiblen Finanzinformationen auf Regierungs-Websites öffentlich zugänglich gemacht wurden. Die Bedrohung für die Sozialhilfeempfänger wird auch dann nicht beseitigt, wenn die Daten nur der Regierung zugänglich sind. Wie die Politikwissenschaftlerin Virginia Eubanks in den USA berichtet, ermöglicht die automatisierte Entscheidungsfindung in der Sozialfürsorge der Regierung, „arme Menschen zu profilieren, polizeilich zu überwachen und zu bestrafen".

Da die Technologie immer weiter voranschreitet, werden diese Bedrohungen noch zunehmen. So kann es beispielsweise die Gesichtserkennungstechnologie Regierungen ermöglichen, Demonstranten, die Sozialhilfe erhalten, anhand der von ihnen zur Verfügung gestellten Digitalfotos zu identifizieren. Malta beispielsweise erwägt bereits den Einsatz von CCTV-Kameras mit Gesichtserkennungssoftware, um „unsoziales Verhalten" zu verhindern. Die mangelnde Berücksichtigung der Privatsphäre und des Datenschutzes in Sozialhilfeprogrammen sollte nicht überraschen. Diese Programme dienen den am stärksten gefährdeten Gruppen – Menschen, die bei der Verteidigung ihrer Rechte bereits benachteiligt sind. Etablierte Stigmatisierung und Vorurteile gegenüber Armen hindern oft andere, privilegiertere Mitglieder der Gesellschaft daran, diese Risiken zu

erkennen, geschweige denn im Namen der Sozialhilfeempfänger zu protestieren. Viele scheinen zu glauben, dass man, wenn man „kostenlose" Leistungen erhält, keinen Datenschutz einfordern kann.

Sozialhilfeprogramme sollen genau das tun, was der Name schon sagt: die bedürftigsten Bevölkerungsgruppen schützen. Die Forderung, dass diese Menschen effektiv auf ihre Rechte auf Privatsphäre und Datenschutz verzichten sollen, ist genau das Gegenteil. Das allein sollte Grund genug sein, sich für die Annahme angemessener Rechtsrahmen, gut ausgestattete Datenschutzbehörden und als letzte Verteidigungslinie eine unabhängige Justiz und Medien einzusetzen. Aber falls manche einen stärkeren Anreiz brauchen: Es gibt immer auch ein Eigeninteresse, denn die Risiken, denen die Schwächsten und Benachteiligten heute ausgesetzt sind, können morgen für einen viel breiteren Teil der Gesellschaft Realität werden.

Aus dem Englischen von Eva Göllner.

(c) Project Syndicate



Magdalena Sepúlveda
Genf

Magdalena Sepúlveda ist Mitglied der Unabhängigen Kommission für die Reform der internationalen Unternehmensbesteuerung (ICRICT) und Geschäftsführerin der Globalen Initiative für wirtschaftliche, soziale und kulturelle Rechte. Zuvor war sie Sonderberichterstatterin der Vereinten Nationen zu extremer Armut und Menschenrechten.