upgrade
democracy

Visions: Demokratie und Technologie

Teil 3

Digitale Identität und Bürgerrechte

Prof. Dr. Thorsten Thiel, Dr. Susanne Kailitz

BertelsmannStiftung

Im Jahr 1993 veröffentlichte die amerikanische Zeitschrift The New Yorker eine Zeichnung von zwei Hunden, die vor einem Computer sitzen. Ein Hund sagt zum anderen: „On the Internet, nobody knows you're a dog". Dieses bis heute berühmte Meme steht für viele immer noch sinnbildlich für das Verhältnis von Kommunikation und Identität im digitalen Raum. Seit 1993 hat sich jedoch viel verändert: Die Fragen, ob wir im Internet im Schutz der Anonymität surfen oder beweisen können, dass wir die Person sind, die wir vorgeben zu sein, sind immer wichtiger geworden. Auch politisch und wirtschaftlich spielen Identifikation und Anonymisierung in digitalen Kontexten eine ungleich wichtigere Rolle. Die Entwicklung wird absehbar dynamisch bleiben – und sie hat Auswirkungen auf die Demokratie, denen wir hier nachgehen wollen.

Worum geht es?

Die Entwicklungen im Bereich digitaler Identität sind vielschichtig. Das liegt nicht zuletzt daran, dass wir zwar einerseits sehen, dass die Anonymität digitaler Kommunikation zwar abgenommen hat. Andererseits haben sich aber bis heute keine übergreifenden Standards für eine digitale Identität durchgesetzt. Wir gehen deshalb davon aus, dass es weitere Versuche geben wird, Identifizierungsverfahren und ein Identitätsmanagement für die digitale Kommunikation zu etablieren. Dabei sind vor allem drei Arten von Identifizierungssystemen von Bedeutung: staatliche, privatwirtschaftliche und dezentrale Systeme.

Staatliche Identitäts- und Authentifizierungsverfahren

In dem Maß, in dem sich die Verwaltung digitalisiert und elektronische Verfahren der Bürgerbeteiligung ausgeweitet werden, werden der Ausbau und die Ausweitung staatlicher Verfahren der Zertifizierung digitaler Identitäten vorangetrieben. Ein einheitliches und möglichst umfangreiches Identitätsverfahren soll hier zu einer deutlichen Beschleunigung und Verbesserung von gesellschaftlichen und politischen Prozessen führen (von der Abgabe der Steuererklärung über das Anmelden eines Autos bis zur elektronischen Patientenakte). Demokratische Staaten versuchen zudem, eine sichere und datenschutzkonforme Identifikation möglich zu machen. Bisher bleibt, allen Anstrengungen zum Trotz, die Akzeptanz der unterschiedlichen verfügbaren Technologien in der deutschen Bevölkerung eher gering. Das liegt weniger an technischen Hindernissen als vielmehr daran, dass diese bisher meist nur isolierte Handlungsoptionen bieten. In anderen Ländern haben sich übergreifende staatliche Identitätssysteme durchgesetzt: teilweise wegen deren hohen Funktionalität (Dänemark, Estland), teilweise wegen eines starken Verpflichtungscharakters (etwa das indische Aadhaar-System). Ein weiterer Bereich, in dem immer stärker staatliche digitale Identitätsverfahren erprobt werden, ist der gesamte Bereich von Einwanderung und Migration. Der Eindruck scheint nicht zu trügen, dass im Umgang mit Ausländer:innen die Bereitschaft, Neues zu erproben und Bedenken hinten anzustellen, ausgeprägter ist als bei den eigenen Staatsbürger:innen. So entsteht hier ein Testfeld für eine Vielzahl von Identitäts- und Identifizierungsverfahren.

Privatwirtschaftliche Identitäts- und Authentifizierungsverfahren

Auch in kommerziellen Kontexten hat die Zuschreibung digitaler Identität seit vielen Jahren stark an Bedeutung gewonnen. Feste und wiederkehrend identifizierbare digitale Identitäten sind in einer datenzentrierten Wirtschaft ein enormer Wert, weil sie beispielsweise das Zuschneiden von Diensten und Angeboten oder die Personalisierung von Werbung erlauben. Im Bereich wirtschaftlicher Identifizierungsverfahren sind zwei große Tendenzen zu beobachten: Zum einen werden isolierte Identitätssysteme – in denen sich Nutzer:innen gegenüber einem einzelnen Dienst oder Anbieter identifizieren – immer stärker abgelöst von föderativen Identitätsverfahren, in denen Identitäten über viele Dienste hinweg nutzbar werden (etwa die Identitätsmanagementsysteme von Google und Apple). Dies wird nochmal verstärkt durch sogenannte digitale Wallets, also Systeme, die mehrere digitale Identitäten vereinen und gemeinsam nutzbar machen. Zweitens werden gerade die großen Plattformen immer besser darin, Identität entlang einer Vielzahl von Beobachtungspunkten zuzuschreiben, also auch unabhängig von einer expliziten Identifizierung, Handeln und Verhalten im Netz zuordnen und kategorisieren zu können.

Dezentrale Identitäts- und Authentifizierungsverfahren

Eine dritte Entwicklungsrichtung, die wir beobachten, sind Identitätsmanagementsysteme, die stärker dezentral angelegt und die in der Forschungsliteratur als Self-Sovereign Identity bezeichnet werden. Diese sind oft, aber nicht zwingend mit den Diskursen um die Blockchain verbunden. Dieser Typ des Identitätsmanagements ist dadurch gekennzeichnet, dass versucht

wird, technische Lösungen zu entwickeln, in denen der Identitätsnachweis nicht durch eine staatliche oder kommerzielle Instanz erfolgt, sondern durch ein Netzwerk von Verifikationsagenten erstellt wird. Weiterhin liegt der Nutzungsschwerpunkt hier stärker auf anonymem oder pseudonymem Handeln. Beim Rückgriff auf die Blockchain sind gerade die proof of work Implementierung, bei der mit großem Rechenaufwand kryptographische Aufgaben gelöst werden müssen, aufgrund ihres enormen Energiebedarfs kritisch zu beurteilen. Sogenannte proof of stake Systeme, bei denen die Verifikationsagenten eine Art Pfand hinterlegen, sind aktuell noch nicht verlässlich genug und müssen ihren geringeren Energiebedarf noch glaubhaft belegen.

Fingerabdruck, Gesichtserkennung oder Iris-Scan – der Trend geht zur Biometrik

Über alle drei Entwicklungsrichtungen hinweg nehmen Bedeutung und Einsatz biometrischer Identifikationsverfahren stark zu. Hier erfolgen die Zuordnung und Verifizierung über biologische Merkmale, denen eine hohe Eindeutigkeit zugeschrieben wird. Das soll Nutzer:innen davor schützen, dass andere ihre Identität übernehmen können, gleichzeitig macht der Verzicht auf Passwörter die Anwendung schneller und komfortabler. Aufgrund der immer stärkeren Durchdringung des öffentlichen Raums mit Sensoren ist zu erwarten, dass diese biometrischen Identifikationsverfahren nach einer Phase der Problematisierung relativ gute Chancen haben, weite Verbreitung zu finden und in einer Vielzahl von Kontexten eingesetzt zu werden. Entscheidend wird hier sein, wie digitale Identitäten und biometrische Identifizierungsverfahren wahrgenommen werden, ob sie als sicher gelten und welche Akteur:innen unter welchen Umständen Zugriff auf Identifizierungsmöglichkeiten erhalten. Klar ist aber auch: je mehr auf biometrische Daten zur Identifikation gesetzt wird, desto größer ist auch das Risiko des Identitätsdiebstahls, da die Daten über nicht-austauschbare Merkmale und oft dezentral gespeichert werden.

Was sind die Potentiale und Risiken?

Für politische Prozesse sind Identifizierungsverfahren oft unverzichtbar. Erst durch die Feststellung von Identität können sowohl Handlungsmöglichkeiten fair verteilt und zugeschrieben als auch Leistungen zugänglich gemacht werden. Dies gilt für die Abgabe der Stimme bei der Wahl genauso wie beim Bezug von Sozialleistungen oder der Besteuerung von Einkommen und Vermögen. Der Staat muss sicher sein und sicherstellen, dass er es mit der richtigen Person zu tun hat. Effektives Handeln des Staates, gerade auch im digitalen Raum, ist somit darauf angewiesen, verlässliche und sichere Identitätsnachweise zu ermöglichen.

Mit wem spreche ich? Identität im öffentlichen Diskurs

Auch mit Blick auf das Vertrauen im öffentlichen Diskurs ist es wichtig, das digitale Gegenüber identifizieren zu können: Dabei geht es zum einen um die Frage, ob ich in einer konkreten Interaktion mit einem echten Menschen oder mit einer Maschine kommuniziere. Zum anderen ist nicht zu vernachlässigen, dass sich häufig – mit bösen Absichten und ohne – Personen als jemand anderes ausgeben. Der Nachweis authentischer persönlicher Accounts beispielsweise in den Sozialen Medien ist somit zentral, unabhängig davon, ob Klarnamen verwendet werden oder nicht. Vertrauen in die Authentizität der Kommunikation und die Verlässlichkeit des öffentlichen Diskurses hängen somit unmittelbar mit Identifikation zusammen.

Selbstbestimmt identifizierbar

Politische Beteiligung bzw. die Möglichkeit, sich geschützt und ohne Angst vor negativen Konsequenzen politisch zu äußern, sind darauf angewiesen, dass es gelingt, Systeme zu etablieren, die einen selbstbestimmten Umgang mit der eigenen Identität erlauben. Diese Systeme, sowohl staatlich initiiert als auch dezentral organisiert, müssten idealerweise die Büger:innen in die Lage versetzen, selbst zu entscheiden, wann sie eindeutig identifizierbar, wann nur pseudonym zuzuordnen und in welchen Fällen auch komplett anonym sind. Individuen dürfen nicht dem Druck ausgesetzt werden, permanent identifizierbar und adressierbar zu sein.

Schutz durch Anonymität und Pseudonymität

Hierin nämlich besteht die Kehrseite starker Identifizierungssysteme: Sie sind in der Lage, den Schutz zu untergraben, den Anonymität und Pseudonymität gewähren. Gerade Minderheiten und marginalisierte Gruppen sind oft auf geschützte Kontexte angewiesen, um überhaupt eine eigene Position und Stimme zu finden oder kollektive Anliegen zu formulieren. Gerade weil digitale Identitäten von vielen körperlichen oder sozialen Zugehörigkeitsmerkmalen abstrahieren, bestünde durch sie im Grunde die Möglichkeit, stärkere Gleichheit in Bezug auf Leistungen oder Beteiligung zu ermöglichen – dies muss jedoch aktiv ermöglicht werden.

Die autoritäre Gefahr permanenter Überwachung

Permanente Überwachungsmöglichkeiten und dauerhaft zuordenbare Verhaltensprofile schränken die Autonomie von Individuen ein. Es ist kein Zufall, dass starke Identitätsregime oft ein Merkmal für sehr asymmetrische, oft antidemokratische und illiberale Kontexte sind und in autoritären Staaten oder Grenz- und Migrationsregimen genutzt werden. Auch das Anwachsen privatwirtschaftlicher Identitätsmanagement-Systeme kann problematisch sein: Hier ist es das Potenzial zu Ungleichbehandlung, dass sowohl Sicherheitsrisiken birgt als auch die private Autonomie der Bürger:innen untergräbt. Diese Tendenz würde sich zudem weiter verschärfen, wenn virtuelle Welten stärker als bisher zur Verfügung stehen würden.

Dort nämlich ist ein noch sehr viel lückenloseres Tracking von Verhalten und biometrischen Informationen möglich.

Unter dem Strich

Solange wir digital kommunizieren, wird digitale Identität ein strukturelles Dauerthema bleiben – und ein permanentes Identifikations- und Verifikationsproblem mit sich führen. Wir sehen, dass Menschen immer weniger in anonymen Kontexten kommunizieren; das führt dazu, dass die Feststellung der Identität eines Menschen jederzeit und auch rückwirkend möglich wird und immer umfangreicher mit Verhaltensdaten verknüpft ist. Mit Blick auf die Demokratie sind diese Effekte ambivalent zu bewerten. Was gebraucht wird, sind Identitätsmanagementsysteme, die es Bürger:innen erlauben, selbst darüber zu entscheiden, wie und in welchem Umfang sie Daten teilen und sich erkennbar machen.

Zum Weiterdenken

- Anke, Jürgen / Richter, Daniel 2023: Digitale Identitäten: Status Quo und Perspektiven, in: HMD Praxis der Wirtschaftsinformatik 60: 2, 261 – 282. *// Überblickartikel, der in verschiedene digitale Identitätskonzepte einführt und insbesondere aus informatischer Perspektive die mögliche Systeme kategorisiert und differenziert.*

- Cheney-Lippold, John 2011: A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control, in: Theory, Culture & Society 28: 6, 164 – 181 *// Open-Access-Artikel, der die Diskussion um sich verändernde Identitäts- und Identifizierungsverfahren früh prägte. 2017 erschien das Buch "We are Data" des selben Autors, welches die Argumente aktualisiert und vertieft.*

- Renieris, Elizabeth M. 2021: Identity in a "Phygital" World: Why the Shift to Machine-Readable Humans Demands Better Digital ID Governance, Centre for International Governance Innovation. *// Meinungsbeitrag, der insbesondere auf die Verschmelzung digitaler und analoger Identitätspraktiken eingeht und darüber die Notwendigkeit besserer Identitätsmanagementsysteme begründet.*

- Thiel, Thorsten 2017: Anonymität und Demokratie, in: Forschungsjournal Soziale Bewegungen 30: 2, 152 – 161. *// Überblicksartikel, der das Konzept von Anonymität erörtert, dessen Entwicklung in digitalen Kontexten beleuchtet und den Zusammenhang zwischen Anonymität / Identität und Demokratie diskutiert.*

Impressum

Bertelsmann Stiftung
Carl-Bertelsmann Straße 256
33311 Gütersloh
www.bertelsmann-stiftung.de

Verantwortlich
Kai Unzicker
Senior Project Manager
Telefon +49 5241 81-81405

kai.unzicker@bertelsmann-stiftung.de
www.bertelsmann-stiftung.de
www.upgradedemocracy.de

Autor:innen
Prof. Dr. Thorsten Thiel, Dr. Susanne Kailitz,
Dr. Kai Unzicker

Gestaltung
nach morgen

Bildnachweise
Montage Cover: © dehweh - stock.adobe.com
Montage Seite 2: © pinkeyes - stock.adobe.com

Zitationshinweis
Thiel, T. und Kailitz, S. (2024) Digitale Identität und Bürgerrechte. *Visions: Demokratie und Technologie / Teil 3*. Bertelsmann Stiftung. Gütersloh.