Schwere Kost
[Lesestoff, der nicht leicht zu verdauen ist.]

FUNCTION CREEP

Wie das langjährige Wunschprojekt der digitalen Identität den Weg auf unsere Smartphones findet.

[Matthias Müller]

Die Verwendung des Covid-Zertifikats ist derzeit auf Statusmeldungen im Zusammenhang mit dem Coronavirus beschränkt. Jedoch sind bestimmte kommerzielle und staatliche Akteure bestrebt, das Covid-Zertifikat in einen digitalen Identitätsnachweis (e-ID) umzuwandeln. Diese Verschiebung ist bereits im Gang und führt einen tiefgreifenden Paradigmenwechsel herbei, der eine dringende gesellschaftliche Debatte erfordert.

Die digitale Identität (e-ID oder elektronische Identität) ist eine digitale Lösung, die es Bürgern ermöglicht, ihre Identität zu beweisen. Sie besteht darin, dass eine eindeutige Kennung mit einer Reihe von digital gespeicherten Attributen verknüpft wird, die wiederum mit Identitätsnachweisen gekoppelt sind. Die e-ID kann verwendet werden, um bestimmte Dokumente einzusehen, aber auch für den Zugang zu Vorteilen und Dienstleistungen, die von Behörden, Banken und anderen Unternehmen angeboten werden, für mobile Dienste und Online-Zahlungen usw. Wie die Europäische Kommission erklärt, kann die e-ID »die eindeutige Identifizierung einer Person gewährleisten und stellt sicher, dass die richtige Dienstleistung für die Person erbracht wird, die tatsächlich Anspruch darauf hat«.

Für ihre Befürworter würde die e-ID ein ganzes Ökosystem von Produkten und Dienstleistungen ermöglichen, das das Leben der Menschen enorm erleichtern würde. Laut der Beratungsfirma PwC, könnten ihre grundlegenden Attribute durch weitere Attribute und Dokumente ergänzt werden (Sozialversicherungsnummer, medizinische Aufzeichnungen, biometrische Informationen, Schulabschlüsse usw.). Sie könnte als »Katalysator der digitalen Transformation« dienen, indem sie bei unzähligen Gelegenheiten des täglichen Lebens zum Einsatz kommt: Eröffnung eines Bankkontos, Aufnahme eines Darlehens, Steuererklärung, Abschluss einer Versicherungspolice, usw. Und nicht zuletzt würde es zu erheblichen Kosteneinsparungen führen. Laut einem Bericht der Unternehmensberatung McKinsey könnte die Ausweitung bzw. die Vervollständigung der digitalen Identifizierung bis 2030 in den fortgeschrittenen Volkswirtschaften einen wirtschaftlichen Wert von 3% des BIP freisetzen, wobei »etwas mehr als die Hälfte des potenziellen wirtschaftlichen Werts auf den Einzelnen entfällt«.

Aber die e-ID wird seit jeher auch von vielen Experten mit grosser Skepsis und mit Vorbehalt betrachtet. Tommy Cooke vom Surveillance Studies Centre der Queen's University in Kanada und Benjamin J. Muller, ausserordentlicher Professor in der Abteilung für Politikwissenschaft am King's University College der University of Western Ontario, sind der Meinung: »Obwohl diese Systeme hochsicher und vertrauenswürdig sein sollen, bergen sie zahlreiche Risiken in Bezug auf Datenschutz und Zugriff«. Sie betonen, dass diese Risiken über Cybersicherheit, verantwortungsvolle Unternehmensführung und organisatorische Verantwortung hinausgehen. Die digitale Identität ist weit mehr als ein elektronischer Personalausweis. Sie wird zwangs-

läufig mit jedem zusätzlichen ‚Service' der an das System übergeben wird zu einer digitalen Biografie, die alle Daten, Transaktionen und Querverbindungen enthält, die wir im Laufe des Lebens ansammeln. Mit jeder Transaktion werden diese Daten geteilt und aktualisiert - und es erfolgt unvermeidlich auch ein Rating der Person (A-Person, B-Person, berechtigte Person, unerwünschte Person, etc.), weil die KI, die diese Daten organisieren muss, versuchen wird, Prognosen für zukünftiges Verhalten der betreffenden Person zu berechnen. Das kann positiv sein, oder auch das Gegenteil. Die Befürworter dieser Technologien lenken den Blick gerne nur auf die möglichen Vorteile, aber wie jede Medaille, so hat auch diese zwei Seiten.

OPFER DER AUSFÄLLE UND VERZERRUNGEN DER SYSTEME

Das indische System Aadhaar ist ein gutes Beispiel für dieses Problem. In Indien ist die e-ID bereits für mehr als eine Milliarde Menschen Realität. Aadhaar ist heute das grösste biometrische Identifikationssystem der Welt. Vom Milliardär Nandan Nilekani mit Unterstützung u. a. von Mastercard geschaffen, verfolgt es die Bewegungen der Nutzer von einer Stadt zur anderen, ihren beruflichen Status und ihre Transaktionen. Aadhaar, das vom damaligen Chefökonomen der Weltbank, Paul Romer, begeistert als »das ausgeklügelte Identifikationsprogramm der Welt« bezeichnet wurde, hat auch Pannen, deren Folgen dramatisch sein können. Recherchen im Jahr 2017 ergaben, dass es zu Todesfällen kam, weil das System diesen Leuten zustehende Essensrationen verweigerte oder ihre Rente fälschlicherweise an jemanden anderen auszahlte. Die Authentifizierung war aufgrund von schlechten Verbindungen, biometrischen Fehlern, Serverproblemen, fehlerhafter Datenverknüpfung, Fehlermeldungen und anderen technischen Fehlern fehlgeschlagen. Die Folge: Im Bundesstaat Jarkhand im Nordwesten des Landes mussten 2,5 Millionen Menschen auf ihre monatliche Getreideration verzichten, weil das System sie ausgeschlossen hatte.

Leider wurde dies nicht korrigiert, um in Zukunft weitere tragische Ausfälle zu vermeiden. Im Gegenteil, erklärte uns Sunita Sheel, Anthropologin und unabhängige Bioethikforscherin aus Mumbai, »die Dinge haben sich durch die Pandemie noch verschlimmert«. »In Indien«, betont sie weiter, »gab es eine starke Lobby, die dieses aggressive Vorgehen des Staates bei der Einführung der digitalen Technologie kritisierte«, aber sie war doch nicht stark genug, um »die Probleme zu ändern, die marginalisierte Gemeinschaften vor Ort erleben, ebenso wie die Mittelschicht«. Heute ist das Aadhaar-Konto einer Person mit allen möglichen Daten und Systemen verknüpft: mit der PAN (Permanent Account Number), dem PDS (Public Distribution System), dem Direct Benefit Transfer (DBT) und ihren Bankkonten. »Selbst die Beschaffung eines neuen Passes ist ohne Aadhaar nicht möglich«, sagt Sunita Sheel. »Auch der Kauf und die Übertragung von Eigentum kann nicht durchgeführt werden, ohne das Aadhaar vorzulegen und mit den entsprechenden Behörden zu teilen.« Auch in Europa kommt es immer wieder zu Ausfällen von Covid-Zertifikaten. Bei jedem Ausfall bleibt den Inhabern der Zertifikate der Zugang zu Orten verwehrt, obwohl diese eigentlich für sie zugänglich wären.

All diese Fälle zeigen ein grosses Problem solcher Systeme auf: Es ist immer zuerst die Person, deren Verifizierung fehlschlägt, die als ‚nicht konform' angesehen wird, obwohl das Scheitern auf einen Fehler oder eine Verzerrung im Design des Systems zurückzuführen sein kann und die Korrektur eines systemischen Fehlers wird aufgrund der speziellen Architektur dieser Monstersysteme zum bürokratischen und technischen Alptraum für jeden Betroffenen.

Die e-ID-Lobbys zementieren unterdessen bestimmte Überzeugungen unter den Entscheidungsträgern. Tommy Cooke und Benjamin J. Muller stellen fest: »Smartphones werden von den Behörden zunehmend als Technologien wahrgenommen, die mehrere Lücken gleichzeitig schliessen können. Nicht nur, um den Eindruck zu beheben, nicht in der Lage zu sein, die öffentliche Sicherheit zu gewährleisten, sondern auch, um wirtschaftliche Schwierigkeiten zu überwinden.« So sind Smartphones, nachdem sie die naheliegenden Träger von Tracking-Apps waren, nun die bevorzugten Träger von Covid-Zertifikaten. »Da Pässe oder Impfbescheinigungen zunehmend als lebenswichtige Funktionen der öffentlichen Sicherheit wahrgenommen werden, sind nun auch privatwirtschaftliche Einrichtungen wie Restaurants, Bars, Fitnessstudios und Clubs dazu verpflichtet, einen Identitäts- und Impfnachweis zu verlangen«, erinnern die kanadischen Forscher noch einmal. Im Laufe der Covid-Krise ist das Smartphone weit mehr als ein einfacher Rechner und Analysewerkzeug geworden. Es ist nun auch ein ‚Wahrheitsträger' im Kontext der Staatsbürgerschaft und des angeblichen Gesundheitszustands. Ebenso wichtig ist, dass es sich auch in ein Vehikel zur Ankurbelung und Stimulierung der Wirtschaft verwandelt.

Im Zuge dieser Verschiebung sind immer mehr Regierungen bereit, auf den Zug aufzuspringen und die e-ID zu realisieren, indem sie die Infrastruktur der Covid-Zertifikate nutzen: »Digitale Identitätssysteme sind auf dem Vormarsch«, bestätigen Cooke und Muller. Kurz vor oder während der Pandemie haben viele Regierungen auf der ganzen Welt (z. B. Grossbritannien, Australien, Neuseeland, die EU, Kanada und andere) angekündigt, dass sie Technologiesysteme entwickeln werden, mit denen Bürger und Organisationen ihre Identität nachweisen können - oder dass sie bereits dabei sind, dies zu tun.

TRANSFORMATION IN DER EU IM GANGE

Die Europäische Kommission beispielsweise äussert nun offen ihren Wunsch, dass sich das Covid-Zertifikat der EU zu einer e-ID-Wallet-Lösung weiterentwickeln soll. Charles Manoury, Sprecher der Europäischen Kommission, erklärte: »Die Vorlagenlösung die den Mitgliedstaaten zur Verfügung gestellt wird, um Anwendungen zur Speicherung von EU-CDCs zu erstellen [EU Covid-Zertifikat, Anm. d. R.], ist die erste Form dessen, was sich zum vollwertigen digitalen Wallet entwickeln kann.«

Als die Europäische Kommission im März 2021 ihre Absicht ankündigte, das Covid-Zertifikat einzuführen, hatte sie ihre Bürger jedoch nicht davor gewarnt, dass das »gemeinsame Modell, das mit den Mitgliedstaaten entwickelt wurde, um die Anerkennung von in Papierform ausgestellten EU-COVID-Zertifikaten zu erleichtern«, zu einem »vollwertigen digitalen Wallet« weiterentwickelt werden soll. Ganz im Gegenteil. Damals behauptete sie, dass Covid-Zertifikate »mit der COVID-19-Pandemie verbunden« seien, und das »System der digitalen grünen Zertifikate« würde »ausgesetzt, sobald die Weltgesundheitsorganisation (WHO) das Ende der durch das COVID-19-Virus verursachten Gesundheitsnotlage erklärt hat« und könne nur reaktiviert werden, »wenn die WHO eine neue Gesundheitsnotlage im Zusammenhang mit COVID-19, einer Variante davon oder einer ähnli-

chen Infektionskrankheit ausruft«. Wie wir alle derzeit erleben müssen, wird die ‚globale Bedrohung' jedoch gerade als Dauerzustand etabliert.

Die Aussicht auf ein Covid-Zertifikat, das sich zu einer »vollwertigen digitalen Brieftasche« entwickelt, widerspricht also diesen Zusicherungen einer begrenzten Nutzung, sowohl zeitlich als auch hinsichtlich des Anwendungsbereichs.

Wie energisch die Interessengruppen sich auch über demokratische Mandate hinweg setzen, beweist die Schweiz. Am 7. März 2021 lehnten 64,4% der Schweizer den ersten Entwurf des e-ID-Gesetzes ab. Nur drei Tage später wurden bereits die ersten Anstrengungen unternommen, um das Thema schnellstmöglich wieder aufzugreifen: Am 10. März 2021 wurden im Parlament sechs Motionen mit identischem Wortlaut eingereicht, die die Einführung eines »ein staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt«, forderten. Die Dinge liessen dann nicht lange auf sich warten und die Konsultation endete bereits am 14. Oktober 2021.

Im Juli 2021 hatte das Lobbying seine Wirkung getan und die Aargauer Zeitung schrieb sinngemäss: »Früher wollte niemand die e-ID, aber Covid hat das Blatt gewendet. Nach eineinhalb Jahren Pandemie ist die digitale Welt in der Schweiz nicht mehr dieselbe wie vor Covid. Die Covid-App und das Covid-Zertifikat, die im gleichen Geist geschaffen wurden, haben eine neue Grundlage geschaffen«, behauptete der Artikel, der die begeisterten Worte des grünen Nationalrats Gerhard Andrey zitierte. Für den IT-Unternehmer hatten die SwissCovid-App und das Covid-Zertifikat »eine völlig neue Dynamik in der Schweiz« ausgelöst und »den politischen Mainstream geprägt«. Kurzum: »Eine ähnlich geprägte e-ID könnte zum Renner werden«, hiess es.

VERKNÜPFUNG VON IMPFSTATUS, BIOMETRISCHEN DATEN UND E-ID

Eines ist sicher: Die Unternehmen und Interessengruppen, die die e-ID durchsetzen wollen, haben nicht nur theoretische Überlegungen angestellt und nicht erst die Covid-Krise abgewartet, um aktiv zu werden, jedoch spielte ihnen die Krise alle Trümpfe in die Hand.

Die »Digital-Identity-Industrie« ist seit Anfang der 2010er Jahre und insbesondere seit 2014 aktiv: In diesem Jahr hat die Weltbank die Initiative Identification for Development »ID4D« ins Leben gerufen. Sie soll Ländern dabei helfen, das Ziel 16.9 der Vereinten Nationen für nachhaltige Entwicklung zu erreichen: »Bis 2030 allen Menschen eine legale Identität zu verschaffen, einschliesslich der Registrierung von Geburten.« Laut der Weltbank soll die Erreichung dieses Ziels »Fortschritte« bei der »Beseitigung der Armut, der Verringerung von Ungleichheiten, der Gleichstellung der Geschlechter und der Stärkung der Frauen, der sicheren und geordneten Migration, der allgemeinen Gesundheitsversorgung und der finanziellen Inklusion« ermöglichen. Die Implementierung der e-ID und ihre potenziellen Anwendungsbereiche in der realen Welt wurden also bereits seit mehreren Jahren getestet, insbesondere in den Ländern der südlichen Hemisphäre.

So geht die Idee, Impfstatus und e-ID zu koppeln, auf das Jahr 2018 zurück. Sie wurde von der ID2020-Allianz vorgestellt, die sich zum Ziel gesetzt hatte, die Tatsache zu nutzen, dass in vielen Entwicklungsländern die Durchimpfungsrate weit über der Geburtenregistrierungsrate liegt. Schätzungen zufolge, so schrieb ID2020, »erhalten mehr als 95% der Kinder weltweit mindestens eine Dosis eines Impfstoffs« und »86% der Kinder weltweit erhalten die empfohlenen drei vollständigen Dosen des Impfstoffs gegen Diphtherie, Tetanus und Keuchhusten, was üblicherweise zur Messung der Durchimpfungsrate verwendet wird«.

Der Vorschlag lautete daher: die Impfung als »Einstiegspunkt« für die Implementierung eines e-ID-Systems zu nutzen, indem der Impfstatus mit einem biometrischen Identifikationssystem verknüpft wird. »Impfungen sind eine grossartige Gelegenheit, Kindern von Beginn ihres Lebens an eine dauerhafte, tragbare und sichere digitale Identität zu verschaffen«, lobt ID2020. Inzwischen wurde das Prinzip im Rahmen eines Projekts in Bangladesh in die Praxis umgesetzt, wo »weniger als 40% der Kinder vor ihrem fünften Lebensjahr eine Geburtsurkunde erhalten«, die Impfrate jedoch »97% für vermeidbare Krankheiten« beträgt. ID2020 verwaltet dort nun die biometrische Registrierung und digitale Identifizierung von Säuglingen, wenn sie Routineimpfungen erhalten. Im September 2019 äussert Seth Berkley, CEO von Gavi, den Wunsch, dass das Programm in Zusammenarbeit mit Akteuren wie Facebook und dem Zahlungsunternehmen Mastercard, das im Bereich der e-ID sehr aktiv ist, auf alle Entwicklungsländer ausgeweitet werde.

Ebenfalls 2018, als ID2020 sein Projekt vorstellte, entschied sich Mastercard für denselben »Einstiegspunkt«, ging zu diesem Zweck eine Partnerschaft mit der Gavi-Allianz ein und trat an Trust Stamp heran, ein auf künstlicher Intelligenz basierendes Unternehmen für Identitätsauthentifizierung. Ziel des Projekts: Aufbau einer Plattform für biometrische Identitäten in abgelegenen Gemeinden mit niedrigem Einkommen in Westafrika. Ausgangspunkt ist der Wellness Pass, ein digitaler Impfpass, der mit einem Identitätsprüfungssystem verbunden ist, das von NuData, der Technologie für künstliche Intelligenz und maschinelles Lernen von Mastercard, gespeist wird. Die von diesen drei Akteuren entwickelte Plattform wurde im Juni 2020 eingeführt, wobei eine von Trust Stamp entwickelte Lösung in den Wellness Pass von Gavi und Mastercard integriert wurde. In beiden Fällen war das Gespenst der Überwachung und des masslosen Absaugens sensibler biometrischer Daten nie sehr weit entfernt.

Die Trust Stamp-Technologie im Mastercard-Projekt beispielsweise ist auch die Technologie, die das Unternehmen Strafverfolgungsbehörden und Gefängnissystemen für die Zwecke der Überwachung und des ‚Predictive Policing' anbietet. Predictive Policing - dieser elegante Fachterminus in bestem Englisch ist nichts anderes, als die Idee, zukünftige Kriminelle anhand ihrer Daten (Biometrik, genetische Informationen, Transaktionen und Sozialverhalten) schon vor einer eventuellen Straftat zu identifizieren, die ‚Wunderwaffe KI' (Künstliche Intelligenz) soll´s richten um aus den Gigatonnen an Daten, die jeder von uns dann tagtäglich in das System einspeist potenzielle Verbrecher auszufiltern und unschädlich zu machen. Für irre Technokraten die Erfüllung eines feuchten Traums, für Realisten eine dystopische Horrorvision.

GHOST-MANAGEMENT AM WERK

Parallel zu diesen Aktivitäten vor Ort haben die verschiedenen interessierten Akteure einen umfangreichen Lobbyapparat aufgebaut, um ihre Agenda voranzutreiben und den Übergang zur e-ID auf möglichst globaler Ebene zu erleichtern. Dieses komplexe Geflecht aus prominenten Gallionsfiguren, Thinktanks und supranationalen Initiativen wird von den Giganten des globalisierten Kapitalismus, Regierungsbehörden, Banken, Kreditinstituten, Zentralbanken, Einrichtun-

Schwere Kost

[Lesestoff, der nicht leicht zu verdauen ist.]

gen, die bei Regierungsbehörden unter Vertrag stehen, Stiftungen von Milliardären, Beratungsfirmen und einer Unzahl von Unternehmen getragen, die sich gegenseitig unterstützen. Viele dieser Akteure gehören zu dem, was Privacy International als »e-ID-Industrie« bezeichnet.

Ihre Schaufenster kommunizieren mit verschwommenen und beschwichtigenden Vokabeln, die die e-ID als Empowerment-Lösungen darstellen, die Vertrauen, Sicherheit, Einfachheit, Komfort, reibungslosen Übergang und vor allem »Inklusion« garantiert: inklusive Entwicklung, inklusive Finanzdienstleistungen, inklusives Wachstum, digitale Inklusion, politische Inklusion, inklusive Technologie, ein bunter Strauß technokratischer Segnungen. Die e-ID sei auch die Schlüsselwaffe gegen den »Identitätsdiebstahl«, dessen Ernsthaftigkeit diese Akteure nicht müde werden zu betonen. Auch an die Emotionen wird appelliert: Wer ist schon so herzlos, dass er sich nicht wünscht, dass alle Neugeborenen mit ID2020, »Zugang zu einem breiteren Spektrum an sozialen Diensten« und »Gesundheitsmassnahmen, die alle Kinder brauchen und verdienen« haben?

Bei all diesen Aufrufen darf man nicht vergessen, dass die e-ID für dieses riesige Konglomerat in erster Linie ein ausserordentlicher Glücksfall ist: für die kommerziellen Akteure in finanzieller Hinsicht und für die staatlichen Akteure in Bezug auf Kontrolle und Überwachung. Die Vertreter des Überwachungskapitalismus, der biometrischen Technologien und des Trackings sind unter ihnen besonders stark vertreten. So gehören zu den enthusiastischsten Unterstützern der Umwandlung von Covid-19 QR-Codes in e-IDs zum Beispiel die Firma Thales, der französische Riese für biometrische Technologien und Überwachung. Oder das britische Unternehmen iProov, das sich auf biometrische Online-Authentifizierung spezialisiert hat.

KRISE ALS BESCHLEUNIGER

Die Covid-Krise hat also einer von einem mächtigen Komplex getragenen Agenda, die seit einem guten Jahrzehnt reift, einen gewaltigen Beschleunigungsschub verliehen. Die Früchte scheinen nun reif für die Ernte zu sein und die Erwartungen sind dementsprechend hoch. Laut dem Marktforschungsunternehmen ‚Mordor Intelligence' (sic!), haben 72% der Online-Marktplätze ihre Technologie zur Identitätsprüfung aufgrund von Covid-19 verstärkt, und die digitale Identitätsprüfung wird immer mehr zu einem wesentlichen Bestandteil des Bankensektors. Laut dem Portal MarketsandMarkets wird der Markt für Lösungen zur digitalen Identität im Jahr 2024 49,5 Mrd. USD schwer sein.

Auch wenn die offensichtlichsten Lobbys der Industrie für digitale Identität vor allem mit privaten Unternehmen und Stiftungen verbunden sind, bedeutet dies nicht, dass die von den Staaten getragenen Lösungen per definitionem unbedenklich sind. Dies gilt auch für die EU.

In ihrer Kommunikation hat die Europäische Kommission vor allem ihren Wunsch hervorgehoben, dass die Einwohner der EU »die Kontrolle« über ihre Daten behalten, »anstatt sie mit Technologiegiganten wie Google und Facebook zu teilen«. Dieser erklärte Wunsch, »die Bürger vor den digitalen Giganten zu schützen«, hat die EU nicht davon abgehalten, in den letzten 15 Jahren Milliarden von Euro in Überwachung und biometrische Technologien zu investieren. Im Dezember 2020 deckte eine Untersuchung von The Guardian auf, dass Horizon 2020, das EU-Forschungsförderungsprogramm, zwischen 2007 und 2020 die Entwicklung von Sicherheitsprodukten für Polizeikräfte und Grenzkontrollbehörden im öffentlichen und privaten Sektor mit 2,7 Milliarden Euro unterstützt hat. Die meisten dieser Produkte nutzten Technologien wie künstliche Intelligenz, Drohnen und Augmented Reality, Gesichts-, Sprach-, Venen- und Iriserkennung sowie andere Formen der Biometrie, die für die Überwachung eingesetzt werden können.

Im Januar 2021 stellte eine Recherche auf voxeurop fest, dass eine wachsende Zahl biometrischer Innovationen, die in jüngster Zeit in verschiedenen europäischen Ländern eingeführt wurden (z. B. biometrische Verifizierung bei der Paketzustellung, Zahlungen per Gesichtserkennung und biometrische Zahlungskarten), in eine zentrale Identität integriert werden könnten. Der Artikel kam zu dem Schluss, dass die Entscheidung, nur digitale Identitäten und Covid-Zertifikate als Mittel für eine »Rückkehr zur Normalität« zu wählen, einem beispiellosen Überwachungssystem Tür und Tor öffnete, durch das die Bürger zudem ihrer Rechte beraubt werden könnten.

Schliesslich ist es sicher, dass private Lobbyisten ihr ganzes Gewicht in die Waagschale werfen werden, um die künftigen Funktionen der EU-e-ID und die Rechtsvorschriften, die den Rahmen dafür bilden, zu beeinflussen. Sie begrüssen zwar die Initiative der Europäischen Kommission, haben aber bereits betont, wie wichtig es ist, die Industrie, den Finanzsektor und das Know-How des Privatsektors in die Gestaltung des endgültigen Systems einzubeziehen.

Die e-ID ist auch das Herzstück eines weiteren Wandels, der von den Bürgern noch nicht wahrgenommen wird, obwohl er weltweit voll im Gange ist: Die Einführung von digitalen Währungen, die von Zentralbanken entwickelt und auch als »Central Bank Digital Currency« (CBDC) bezeichnet werden. Derzeit arbeiten rund 120 Länder der Erde - zufällig genau die Länder, die durch Endlosschleifen von „Wellen", „Lockdowns" und „Maßnahmen" aufgrund von „Virusvarianten" offensichtlich Zeit gewinnen müssen - an der Umsetzung von CBDC-Plänen.

Langfristig sollen die derzeitigen Währungen in digitale Zentralbankwährungen umgewandelt werden, um Kryptowährungen wie Bitcoin entgegenzuwirken, die im libertären Geist und mit dem Ziel eingeführt wurden, dass die Nutzer sich von den Banken befreien und eine neue gemeinschaftliche Währungsordnung einführen können. So wurde die Einführung eines digitalen Euros bis spätestens 2025 im September 2021 von der EZB angekündigt.

Die Vorteile von CBDCs werden als wichtig, praktisch und wünschenswert dargestellt. Kostensenkung, Erleichterung des Zahlungsverkehrs, Bekämpfung von Geldwäsche und Korruption, Übergang zu einer bargeldlosen Wirtschaft und Förderung der finanziellen Eingliederung. Wie wir schon bei der Argumentation für die digitale ID gesehen haben, wird auch hier der Begriff »Inklusion« als ein Hauptpunkt eingebracht, der diese Entwicklung rechtfertigen soll.

Doch das CBDC-System hat auch eine dunkle Seite, die Kontrolle, Massenüberwachung und Infantilisierung der Bevölkerung miteinander verbindet. Der berühmte Whistleblower Edward Snowden fasste das Problem wie folgt zusammen: »Die CBDC ist eher eine Perversion der Kryptowährung, oder zumindest der Gründungsprinzipien und Protokolle der Kryptowährung – eine kryptofaschistische Währung, ein böser Zwilling, der ausdrücklich dazu bestimmt ist, seinen Nutzern das grundlegende Eigentumsrecht an ihrem eigenen Geld zu verweigern und den Staat als vermittelndes Zentrum jeder

Schwere Kost

[Lesestoff, der nicht leicht zu verdauen ist.]

Transaktion zu installieren«. Das Problem ist, dass kaum ein Bürger tatsächlich versteht, was CBDCs können, bzw. worin der Unterschied zur normalen Kredit- oder Debitkarte liegt. Bei normalen Zahlungssystemen, handelt es sich, auch wenn sie digital abgewickelt werden, immer noch um das eigene Geld, das durch einen Zahlungsauftrag zwischen den Menschen übertragen wird. Bei CBDCs handelt es sich jedoch um „intelligentes Geld", das programmiert werden kann und damit seinen „eigenen Willen" besitzt. Es ist nicht möglich, dieses Geld für „illegale" Transaktionen zu verwenden - was auch immer die jeweilige Regierung dann darunter verstehen möchte.

Sobald sie mit Konten verknüpft wären, die wiederum mit einer e-ID verbunden wären, würden CBDCs alle Transaktionen völlig transparent machen und die Anonymität, die Bargeld garantiert, endgültig aufheben. Zudem würden diese CBDCs wirksam jede Form der Kapitalflucht verhindern und somit den Banken und Regierungen keinerlei Schranken mehr in den Weg stellen, eine toxische Fiskalpolitik zu betreiben.

Die Tatsache, dass CBDCs programmierbar sind, verleihe der Regierung eine enorme Macht, erinnert Laura Dodsworth, Journalistin und Autorin: »Mit CBDCs könnte die Regierung durch die Sammlung von Echtzeitdaten alles darüber erfahren, wie Sie Ihr Geld ausgeben.«

Dieses Szenario ist in China bereits Realität, wo der digitale Yuan derzeit in mehreren Städten getestet wird und die Kontrolle über alle Transaktionen ermöglicht.

TECHNOLOGISCHE GRENZEN

Das Risiko eines »function creep« des Covid-Zertifikats hängt nicht nur mit der Macht und dem Appetit der Akteure zusammen, die versuchen, e-ID und CBDC in den Industrieländern durchzusetzen. Denn auch wenn die Regierungen ihre eigenen, nicht proprietären (Open Source) Lösungen entwickeln, ziehen sie den Einsatz derselben technologischen Lösungen in Betracht, insbesondere der Public Key Infrastructure (PKI) und der Self Souvereign Identity (SSI), die den Einsatz der Blockchain voraussetzen.

Nun gibt es aber viele Missverständnisse, sowohl darüber, was diese Technologien können, als auch über ihre Ausgereiftheit. Wenn Stimmen laut werden und vor den Risiken warnen, welche die Covid-Zertifikate als Überwachungsinstrument darstellen, sowie vor der Bedrohung, die sie für die Privatsphäre und die persönlichen Freiheiten darstellen, wird immer wieder eine Antwort gegeben: Aufgrund ihrer Natur und ihrer Architektur würden die verwendeten Technologien den Schutz der Privatsphäre, die Sicherheit und die Gewissheit, dass jeder die Kontrolle über seine persönlichen Daten behalten kann, aus sich heraus gewährleisten.

In Wirklichkeit sind solche Zusicherungen bestenfalls verfrüht und schlimmstenfalls bewusst irreführend, da sie eine ganze Reihe von entscheidenden Aspekten ausser Acht lassen. Bisher hat diese Technologie nämlich noch keines dieser Versprechen eingelöst. »Relativ junger Ansatz, einige Grundsatzfragen sind noch nicht geklärt und Standards sind noch nicht definiert«, heisst es im schweizerischen »Diskussionspapier zum Zielbild e-ID«. Ausserdem kann niemand von uns die Zukunft vorhersagen: Wie in der Recherche zur ID2020 Alliance des öffentlich-rechtlichen Schweizer Fernsehens SRF festgestellt wurde, kann niemand sagen, welche Techniken Hacker in der Zukunft anwenden werden, auch wenn die neuen Technologien heute unangreifbar erscheinen. Ausserdem haben alle Computersysteme Hintertüren, durch die sich die Geheimdienste der Industrieländer Zugang verschaffen.

SIE VERGISST NICHTS UND IST DEZENTRALISIERT. IST DIE BLOCKCHAIN WIRKLICH EINE GUTE SACHE?

Auch die Blockchain ist in aller Munde, wenn es um die e-ID geht: Sie soll Dezentralisierung garantieren und inhärent sicher sein. Diese Behauptungen verschleiern, dass Blockchain eigentlich eine Buchhaltungstechnologie ist. Und als solche erstellt sie permanente Protokolle, wie auf dem Portal Coingape.com erklärt wird: »Die Blockchain ist im Wesentlichen ein offenes und verteiltes Haupt-Protokoll, das Transaktionen dauerhaft und überprüfbar aufzeichnen kann. Die Blockchain ist resistent gegen die Veränderung von Daten, was sie zu einem hervorragenden Kandidaten für den Schutz und die Sicherung von Protokollen macht.« Aber ist es wirklich was wir wollen im Zusammenhang mit einer digitalen Identität? Ein permanentes Transaktionsprotokoll, wo für immer und alle Zeit festgehalten wird, wer wann wo was gemacht hat?

Elizabeth Renieris ist Technologie- und Menschenrechtsexpertin am Carr Center for Human Rights Policy der Harvard Kennedy School of Government, Praktikerin am Digital Civil Society Lab der Stanford University und Gründungsdirektorin des Notre Dame-IBM Technology Ethics Lab an der University of Notre Dame, Indiana. In einem vor kurzem veröffentlichten Artikel bezweifelte sie, dass dies der Fall ist, da »die Blockchain als dauerhafte und unveränderliche digitale Aufzeichnung gedacht ist« und deswegen, »von Natur aus im Widerspruch zum Grundsatz der Speicherbegrenzung« steht. Elizabeth Renieris verliess ID2020 im Mai 2020, als die Allianz begann, die Blockchain für Covid-Zertifikate zu propagieren.

Tatsächlich steht diese vollständige Rückverfolgbarkeit beispielsweise im Konflikt mit dem Datenschutzrecht in der EU. Nach der Europäischen Datenschutzverordnung (DSGVO) müssen personenbezogene Daten gelöscht werden, sobald der Zweck ihrer Erhebung entfällt oder die betroffenen Personen ihre Einwilligung widerrufen. Eine solche Löschung ist in der Blockchain prinzipbedingt nicht möglich.

Ein weiteres Missverständnis ist, dass die Blockchain als dezentral per Definition dargestellt wird, was angeblich einen entscheidenden Vorteil für den Datenschutz im Vergleich zu einem zentralisierten System darstellt. Für Paul Oude Luttighuis, Berater für Informationsarchitektur in den Niederlanden, ist dies eine unzutreffende Beschreibung. Denn der Inhalt einer Blockchain lässt sich nur sehr schwer ändern: »In einer Demokratie«, betont er, »sind es die Menschen, die einen menschlichen Vertrag mittels eines politischen Prozesses aufsetzen. Der Vertrag kann also geändert werden«. Aber im Fall der Blockchain »ist es eine formale Logik, ein Softwarecode, bei dem niemand da ist, um zu diskutieren, anzupassen oder Änderungen vorzunehmen. Sobald alle in diese Blockchain involviert sind, sobald ihre Verbreitung wächst, sind Änderungen fast unmöglich. Es gibt kaum Spielraum für Veränderungen. Wir schliessen uns gegenseitig in einen nicht anpassungsfähigen sozialen Vertrag ein«. Mit anderen Worten: Sobald die Technologie einmal etabliert ist, wird jede Form der menschlichen Koordination ausgeschaltet. Das bedeutet, das Prozesse, die einmal in dem System als Standard programmiert sind, nachträglich nicht mehr verändert werden können, selbst wenn sie sich für alle Beteiligten als untauglich erweisen.

In der Tat, so Paul Oude Luttighuis,

Schwere Kost

[Lesestoff, der nicht leicht zu verdauen ist.]

»ist die Blockchain in ihrem ultimativen Konzept ein trojanisches Pferd. Sie gibt vor, ein praktisches Werkzeug für unsere Bedürfnisse zu sein – oft unter Verweis auf unsere Angst und unser Misstrauen – aber von innen heraus nagt sie am Leben einer Demokratie und der Rechtsstaatlichkeit. Das sind grosse Worte, und eine isolierte Umsetzung der Blockchain wird sicherlich nicht so verheerende Auswirkungen haben. Aber das Konzept der Blockchain mit seiner Architektur induziert diese Effekte, insbesondere wenn es in grossem Massstab in der Regierungsführung eingesetzt wird«.

TECHNISCHER SOLUTIONISMUS

Die Rechtfertigung dieser Systeme begann im Kontext der inneren Sicherheit – einem Kontext, der traditionell davon absieht, die Öffentlichkeit einzubeziehen, erinnern Tommy Cooke und Benjamin J. Muller. Für sie ist die Tendenz der Regierungen, die öffentliche Konsultation zu umgehen, zum Teil auf den ‚technologischen Solutionismus' zurückzuführen. Dieses Glaubenssystem, so die Forscher, postuliert nämlich, dass »die meisten Probleme – seien sie politischer, sozialer, kultureller, wirtschaftlicher oder sonstiger Art – durch Technologie, Algorithmen, und vor allem durch das neue Allheilmittel ‚KI' gelöst werden könnten«.

Diese Ideologie, die auf die Befürworter der e-ID einen solch unwiderstehlichen Reiz ausübt, oktroyiert aber eine reduktionistische und vereinfachte Argumentation, welche die Realität der Interaktionen und Machtverhältnisse ignoriert. Denn selbst bei einem System das theoretisch garantieren würde, dass der Bürger die Kontrolle darüber behält was er über seine Identität preisgibt – wie es der Hype um die souveräne Identität oder SSI verspricht – bringt uns die Realität allzu oft in asymmetrische Situationen, in denen wir keine andere Wahl haben als die Daten preis zu geben, die von uns verlangt werden: beim Grenzübertritt, in unseren Beziehungen zu Behörden, Bankinstituten, Versicherungen, dem Vermieter unserer Wohnung, unserem Arbeitgeber usw. Haben Sie schon einmal darüber nachgedacht, den Softwarelizenzvertrag für Ihr neues iPhone NICHT zu akzeptieren? Das ist es, was eine „asymmetrische Beziehung" ist. Wenn die Anbieter von Infrastruktur und Technologie, die zur Teilnahme am öffentlichen Leben notwendig sind, Bedingungen zu ihrem einseitigen Vorteil formulieren, dann sind formale Rechte bedeutungslos.

Für Elizabeth Renieris, Wirtschaftsanwältin und Expertin für diese Technologien, ist die Idee des Dateneigentums an sich schon falsch, da sie das, was ein universelles Menschenrecht sein sollte, in ein Eigentumsrecht umwandelt.

Nun macht dieses Modell, das postuliert, dass man seine eigenen Daten »besitzt«, diese Daten zu etwas, das möglicherweise auch „freiwillig" verkauft oder gegen etwas anderes eingetauscht werden kann. SSI und die dezentralisierte Identifizierung legen die gesamte Verantwortung auf den Einzelnen: »Die Idee dahinter ist zum Teil, dass man selbst entscheiden kann, seine Daten anderen zur Verfügung zu stellen und dabei die Kontrolle über sie abzugeben«, erklärte sie. »Das mag nach einer Möglichkeit klingen, den Verbrauchern mehr Macht zu geben, vor allem in einer Zeit, in der wir uns alle noch hilfloser fühlen als sonst. Aber da Technologieunternehmen nichts lieber tun würden, als Ihre Daten zu besitzen, werden sie alle möglichen Tricks anwenden, um Sie zur ‚freiwilligen' Preisgabe ihrer Daten zu manipulieren.«

Wie Elizabeth Renieris im April 2021 feststellte, müssen die Covid-Zertifikate in diesem »breiteren Kontext einer beschleunigten Einführung der digitalen Identität« betrachtet werden, mit dem Risiko, dass die als Reaktion auf die Covid-Krise aufgebaute und eingesetzte Infrastruktur für die digitale Identität zu einer dauerhaften Einrichtung wird. »Um diese Bedenken zu zerstreuen, versprechen einige Regierungen, dass die Lösungen nur vorübergehend sind«, stellt sie fest. Die Europäische Kommission erklärte beispielsweise: »Das System der digitalen grünen Zertifikate ist eine vorübergehende Massnahme, die ausgesetzt wird, sobald die Weltgesundheitsorganisation (WHO) den internationalen Gesundheitsnotstand für beendet erklärt. Also nie.«

Auch Tommy Cooke und Benjamin J. Muller sehen eine »auffällig starke Korrelation« zwischen der Entstehung von Impfzertifikaten und -pässen einerseits und digitalen Identitätssystemen andererseits: »Die Art und Weise, wie Regierungen auf der ganzen Welt digitale Identitätssysteme diskutieren und planen, legt nahe, dass Impfzertifikate und -pässe Prototypen für die zukünftige Plattform der digitalen Identität sein könnten.« Doch während die Bevölkerung in der Lage sein sollte, diese Fragen unzensiert zu diskutieren und dabei ehrliche und präzise Erklärungen zu erhalten, muss man feststellen, dass dies in dem derzeit herrschenden toxischen Klima völlig unmöglich ist.

Cooke und Muller betonen: »Wer Sie sind, Ihr Gesundheitszustand und Ihre Fähigkeit, an der Weltwirtschaft teilzunehmen, sind Aspekte, die zunehmend von Ihrem Smartphone abhängen. Die Hintergrundprozesse dieser Anwendungen – diejenigen, die für die Erstellung, Überprüfung und Verteilung von Impfbescheinigungen und/oder digitalen Pässen verantwortlich sind – führen zu beispiellosen Unsicherheiten hinsichtlich der Privatsphäre und des Zugangs für die Bürger. Wer baut, wartet und verwaltet diese Netzwerke? Welche Cybersicherheitsstandards werden verwendet? Welche Arten von Daten, Metriken und anderen Analysen mit sekundärem Nutzen werden in diesen Netzwerken verwendet, von wem und warum? Ist ihr Code Open-Source und wenn ja, wer ist für die Prüfung verantwortlich, um sicherzustellen, dass sie nicht nur gesetzeskonform, sondern auch ethisch verantwortlich sind? Noch wichtiger sind Fragen zur Zukunft: Was bedeutet es, wenn all dies auf mobilen Technologien beruht, die immer verbunden und immer aktiv sind? Wie werden diese Entwicklungen die Art der Beziehungen zwischen öffentlichen und privaten Einrichtungen verändern? Wie lange werden diese Systeme funktionieren dürfen und wie gross werden sie sein? Werden die Bürger zum Beispiel andere Formen von Identitäten auf ihren Smartphones behalten können?«

Nur wenn die Bürger die Möglichkeit haben, diese Aspekte zu prüfen und Antworten in gutem Glauben erhalten, haben sie die Grundlage für eine informierte Entscheidung, ob sie diese Entwicklungen mittragen möchten - oder ob sie im Gegenteil in diesen Plänen eine beunruhigende Entwicklung sehen, weil die bisherige Verwendung des QR-Codes »zur Bekämpfung von Covid-19« ihnen einen Vorgeschmack auf das gegeben hat, was sie in noch grösserem Massstab erwartet. Und dann stimmen sie mit der australischen Journalistin Caitlin Johnstone überein: »Kein normaler Mensch will, dass Gesetze zur digitalen Identität verabschiedet werden. Normale Menschen sitzen nicht herum und sagen: 'Mann, es ist echt scheisse, dass wir unsere Identität nicht online mit einem digitalen Ausweis nachweisen können, der alle unsere Daten enthält.' Nur Konzerne und Regierungen wollen das, und das aus gutem Grund.«