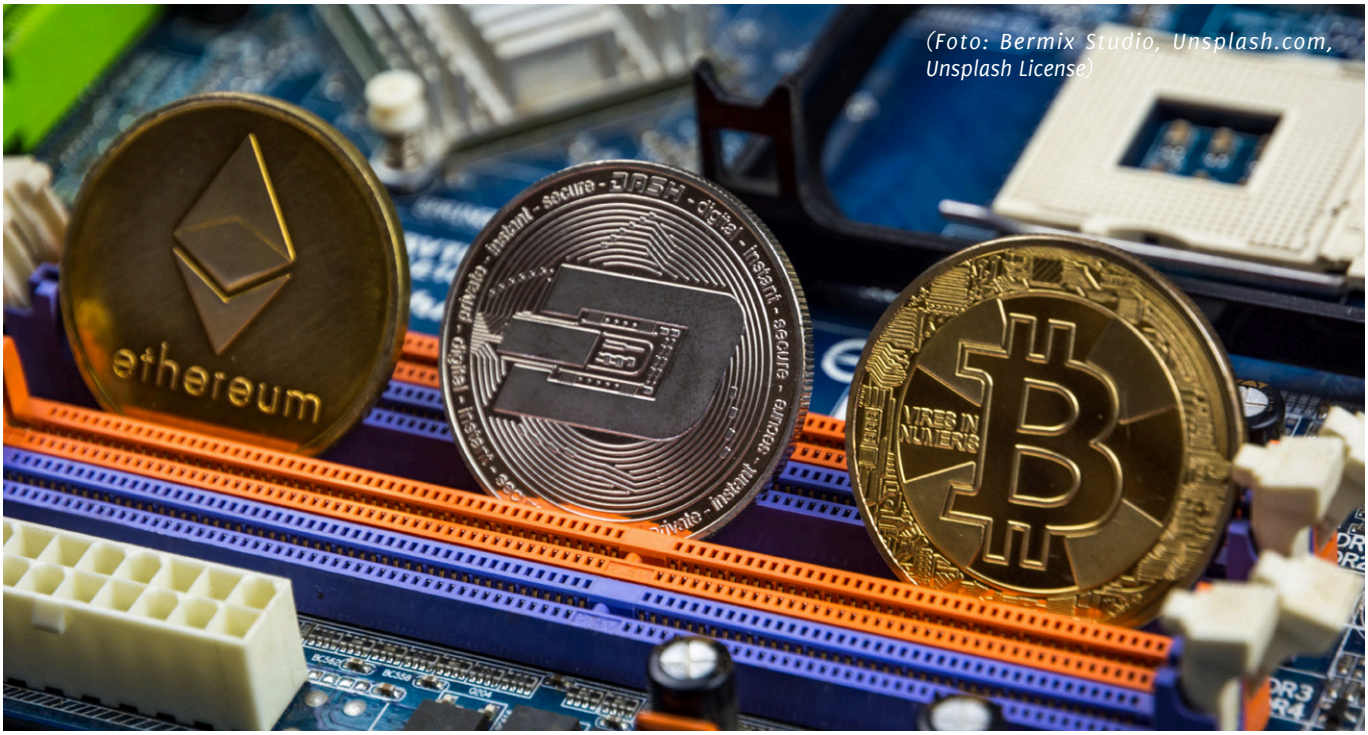


(Foto: Bermix Studio, Unsplash.com, Unsplash License)

„Function creep“ im Pandemie-Modus (3/3):

Der seltsame Fall der **Covid-19-Zertifikate**

In den beiden vorangehenden Episoden [1] [2] haben wir gezeigt, dass die Einführung von Covid-19-Zertifikaten eine willkommene Gelegenheit darstellt, welche von mächtigen Interessengruppen zu nutzen versucht wird, um die Einführung einer Brieftasche (Wallet) für digitale Identitäten (e-ID) zu beschleunigen. Nach den Ausführungen über die Lobbyarbeit, mit der diese Interessengruppen ihre Agenda vorangetrieben haben, ist es nun an der Zeit den Blick auf eine Kategorie von Akteuren zu fokussieren, die ebenfalls auf den Zug aufspringen wollen: die Zentralbanken.

Dritte Folge: Die e-ID und die Kryptowährungen der Zentralbanken

Die e-ID ist das Herzstück eines Wandels, der von den Bürgern noch nicht wahrgenommen wird, obwohl er weltweit im Gange ist: Die Einführung von digitalen Währungen, die von Zentralbanken entwickelt und auch als „central bank digital currency“ (CBDC) bezeichnet werden.

Viele Beobachter sind der Meinung, dass die Zentralbanken vor allem aufgrund der Beschleunigung der Finanzprojekte der GAFAMs (Google (Alphabet), Apple, Facebook (Meta), Amazon und Microsoft), insbesondere des 2019 von Facebook initiierten Projekts Diem (ehemals Libra), welches auf die Schaffung einer stabilen, währungsgestützten Kryptowährung abzielt, in diese Richtung voranschreiten [3].

Dieser Text wurde zuerst am 26.11.2021 auf www.re-check.ch unter der URL ‹https://www.re-check.ch/wordpress/fr/function-creep-covid-19-zertifikate-03/› veröffentlicht.

Im Zusammenhang mit der Covid-Krise wurden die Bürger in vielen Ländern aufgefordert, möglichst kontaktlos zu bezahlen, um Banknoten nicht durch die Hände gehen zu lassen, obwohl keine Studie jemals gezeigt hat, dass es für die Bevölkerung besser ist, diese Zahlungsmethode zu verwenden, als mit Bargeld zu bezahlen. (Foto: Nathan Dumlao, Unsplash.com, Unsplash License)

Langfristig sollen die derzeitigen Währungen in digitale Zentralbankwährungen umgewandelt werden [4], 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 2025 im September 2021 angekündigt [5].

Die Vorteile von CBDCs werden als wichtig, praktisch und wünschenswert dargestellt [6]. Kostensenkung, Erleichterung des Zahlungsverkehrs, Bekämpfung von Geldwäsche und Korruption, Übergang zu einer bargeldlosen Wirtschaft und Förderung der finanziellen Eingliederung. Wie wir in der zweiten Episode [7] 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 Geld zu verweigern und den Staat als vermittelndes Zentrum jeder Transaktion zu installieren“ [8].

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. Dieser Aspekt wurde von vielen Beobachtern im Jahr 2020 hervorgehoben, als die Bürger in vielen Ländern aufgefordert wurden, ihre Einkäufe künftig mit Debit- und Kreditkarten zu bezahlen, möglichst kontaktlos, um „das Hantieren mit Banknoten zu vermeiden“, obwohl keine Studie jemals gezeigt hat, dass es für die Bevölkerung besser ist, diese Zahlungsmethode zu verwenden, als mit Bargeld zu bezahlen.

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.“ [9]

Dieses Szenario ist in China bereits Realität, wo der digitale Yuan derzeit in mehreren Städten getestet wird und die Kontrolle über alle Transaktionen ermöglicht. Wie die westlichen Befürworter einer bargeldlosen Gesellschaft, argumentieren auch die chinesischen Behörden, dass „Bargeld leicht zu fälschen ist und aufgrund seiner Anonymität für illegale Zwecke verwendet werden kann“. Aber es „gibt immer noch Grauzonen über den Besitz und die Verwendung dieses Yuan“, stellte das Journal du Net fest [10]. „Die chinesische Zentralbank PBOC erklärte, dass die Geschäftsbanken bereits über die Infrastruktur verfügten, um diese Währung zu verteilen, was impliziert, dass sie dies wahrscheinlich tun werden, und nicht die Zentralbank. Es gibt auch keine Hinweise auf die Form, obwohl man sich vorstellen kann, dass der QR-Code angesichts seiner Beliebtheit in China eine große Chance hat, beibehalten zu werden.“

Technologische Grenzen

Das Risiko eines „function creep“ des Covid-19-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) [11] und der Self Souvereign Identity (SSI) [12, 13], die den Einsatz der Blockchain [14] voraussetzen. Dies ist in der Schweiz der Fall, wie aus dem Arbeitspapier hervorgeht, das 2021 im Rahmen der Konsultation zum neuen e-ID-Projekt vorgelegt wurde [15].

Nun gibt es aber viele Missverständnisse, die weiterbestehen werden, sowohl darüber, was diese Technologien können, als auch über ihre Ausgereiftheit. Wenn Stimmen laut werden und vor den Risiken warnen, welche die Covid-19-Zertifikate als Überwachungsinstrument darstellen, sowie vor der Bedrohung, die sie für die Privatsphäre und die persönlichen Freiheiten darstellen [16], 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 [17].

Das ist es, was das populäre Konzept der „selbstbestimmten digitalen Identität“ (Self-Sovereign Identity) oder SSI

Publiziert auf Free21 am 04.01.2022, 6:00 Uhr

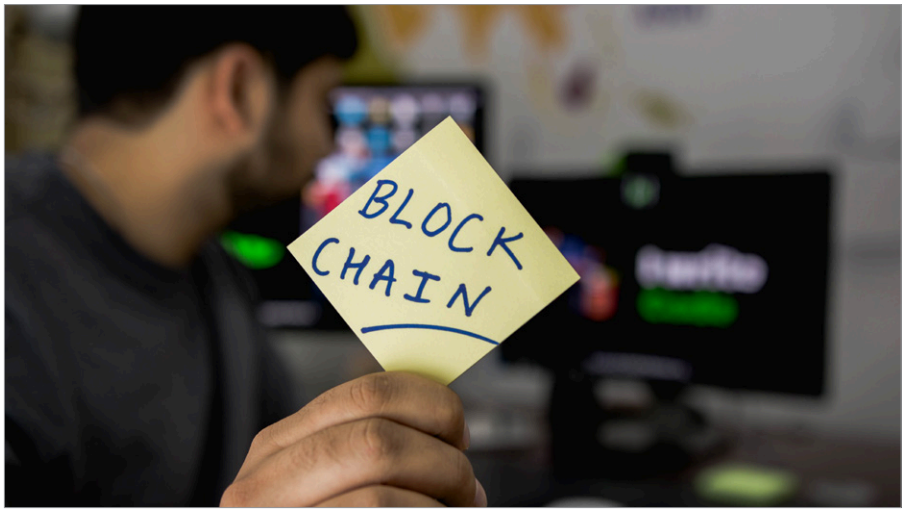
[18], verspricht. „Der Vorteil von SSI: Ähnlich wie die Covid-App bleibt die Hoheit über die eigenen Daten bei den Nutzern“, fasste die Aargauer Zeitung im Juli 2021 zusammen [19]. Die Erklärung: „SSI ist dezentral, die Nutzerinnen und Nutzer sind nicht von einem zentralen Identitätsdienstleister abhängig. Sie verwalten ihre digitalen Identitäten selbst. Persönliche Identitätsmerkmale wie Name, Vorname oder Geburtsdatum werden in einer elektronischen Brieftasche (‚Wallet‘) auf dem Handy hinterlegt. Der Staat als vertrauenswürdige Stelle bestätigt sie. Das sind ‚Verified Credentials‘.“

In Wirklichkeit sind solche Zusicherungen bestenfalls verfrüht und schlimmstenfalls 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 abschließend geklärt und Standards sind noch nicht komplett», heißt es im «Diskussionspapier zum ‘Zielbild E-ID’» (Download nur mit Zugriffsrechten – Anm.d.Red.) im Kapitel über die SSI. Oder: «Die Verantwortung zur Verwaltung von Verified Credentials wird vollständig dem User übergeben, was Hilfeleistungen durch den Issuer praktisch verunmöglicht.» Und:

> Dies kann beim Missbrauchsfall der E-ID oder anderen Nachweisen dazu führen, dass es schwierig wird nachzuweisen, dass man etwas ‘nicht gewesen’ ist.“

Entspricht dies wirklich der Vorstellung einer sicheren e-ID, bei der man «Herr seiner eigenen Daten» ist?

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.



Die Verwendung der Blockchain in Verbindung mit der digitalen Identität funktioniert als dauerhafte und unveränderliche digitale Aufzeichnung und steht damit im Konflikt mit dem Datenschutzrecht in der EU, das eine Möglichkeit zur Datenlöschung vorschreibt (Foto: Hitesh Choudhary, Unsplash.com, Unsplash License)

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 die Blockchain eine „Buchhaltungstechnologie“ ist [20]. Und als solche erstellt sie permanente Protokolle, wie auf dem Portal Coingape.com erklärt wird [21]: „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 und nachvollziehbares Transaktionsprotokoll, wo steht wer was macht, wo und wann?

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 [22]. Elizabeth Renieris verließ ID2020 im Mai 2020, als die Allianz begann, die Blockchain für Covid-19-Zertifikate zu propagieren [23].

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 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 [24]. 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 Ver-

Quellen:

[1] Re-Check, Catherine Riva, Serena Tinari, Jannes van Roermund „«Function creep» im Pandemie-Modus: der seltsame Fall der Covid-19-Zertifikate (1/3)“, am 30.12.2021, <*https://free21.org/der-seltsame-fall-der-covid-19-zertifikate/*>

[2] Re-Check, Catherine Riva, Serena Tinari, Jannes van Roermund „«Function creep» im Pandemie-Modus: der seltsame Fall der Covid-19-Zertifikate (2/3)“, am 02.01.2022, <*https://free21.org/der-seltsame-fall-der-covid-19-zertifikate-2/*>

[3] JDN, Charlie Perreau „Les CBDC, les cryptomonnaies des banques centrales, sont aussi en plein boom“, am 23.04.2021, <*https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1500403-cbdc-definition-euro-numerique-yuan-digital/*>

[4] L'Est Républicain, U.M. „Cryptomonnaies: les Etats et les banques s'y mettent“, am 30.10.2021, <*https://www.estrepublicain.fr/economie/2021/10/30/cryptomonnaies-les-etats-et-les-banques-s-y-mettent*>

[5] Business Insider France, Thomas Chenel „Comment l'euro numérique pourrait tuer certaines cryptomonnaies“, am 10.09.2021, <*https://www.businessinsider.fr/comment-leuro-numerique-pourrait-tuer-certaines-cryptomonnaies-188579*>

[6] European Central Bank, Speech by Fabio Panetta „Central bank digital currencies: a monetary anchor for digital innovation“, 05.11.2021, <*https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211105~08781cb638.en.html*>

[7] Re-Check, Catherine Riva, Serena Tinari, Jannes van Roermund „«Function creep» im Pandemie-Modus: der seltsame Fall der Covid-19-Zertifikate (2/3)“, am 02.01.2022, <*https://free21.org/der-seltsame-fall-der-covid-19-zertifikate-2/*>

[8] Substack Continuing Ed, Edward Snowden „Your Money AND Your Life“, am 09.10.2021, <*https://edwardsnowden.substack.com/p/cbdcs*>

[9] Substack, Laura Dodsworth „All that glitters is not gold… Especially when it's a government surveillance coin.“, am 28.10.2021, <*https://lauradodsworth.substack.com/p/all-that-glitters-is-not-gold-especially*>

[10] JDN, Charlie Perreau „Les CBDC, les cryptomonnaies des banques centrales, sont aussi en plein boom“, am 23.04.2021, <*https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1500403-cbdc-definition-euro-numerique-yuan-digital/*>

[11] Schweizerische Eidgenossenschaft - Bundesamt für Informatik und Telekommunikation BIT „Swiss Government PKI“, <*https://www.bit.admin.ch/bit/de/home/subsites/allgemeines-zur-swiss-government-pki.html*>

[12] Le Temps, Antoine Verdon „Une identité numérique souveraine“, am 16.11.2018, <*https://www.letemps.ch/economie/une-identite-numerique-souveraine*>

[13] Sovrin Foundation „What is self-sovereign Identity?“, am 06.12.2018, <*https://sovrin.org/faq/what-is-self-sovereign-identity/*>

[14] Schweizerische Eidgenossenschaft – KMU-Portal „Sharing mit der Blockchain“, am 04.11.2021 (letzte Änderung), <*https://www.kmu.admin.ch/kmu/de/home/fakten-trends/blockchain.html*>

[15] Schweizerische Eidgenossenschaft – Bundesamt für Justiz „Öffentliche Konsultation zum „Zielbild E-ID““, am 16.11.2021 (letzte Änderung), <*https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/zielbild-e-id.html*>

[16] BNN Bloomberg, Ann Cavoukian „Vaccine passports to create ‚appalling' level of surveillance tracking: Former Ontario privacy watchdog“, am 16.09.2021, <*https://www.bnnbloomberg.ca/canada/video/vaccine-passports-to-create-appalling-level-of-surveillance-tracking-former-ontario-privacy-watchdog~2282674*>

trag 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 ist wie ein Kartenhaus. 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.“

In der Tat, so Paul Oude Luttighuis,

> 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 vom Surveillance Studies Centre der Queen's University und Benjamin J. Muller vom King's University College der University of Western Ontario. 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, Data Mining usw. ‚gelöst' werden können“.

Diese Ideologie [25], die die Befürworter der e-ID so verführt, oktroyiert aber eine reduktionistische und vereinfachte Argumentation, welche die Realität der Interaktionen und Machtverhältnisse zu ignorieren scheint. 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 Dokumente und Informationen vorzulegen, die von uns verlangt werden: beim Grenzübertritt, in unseren Beziehungen zu Behörden, Bankinstituten, Versicherungen, dem Vermieter unserer Wohnung, unserem Arbeitgeber usw.

Für Elizabeth Renieris, Wirtschaftsanwältin und Expertin für diese Technologien, ist die Idee des Dateneigentums an sich falsch, da sie das, was ein universelles Menschenrecht sein sollte, in ein Eigentumsrecht umwandelt [26, 27]. Nun macht dieses Modell, das postuliert, dass man seine eigenen Daten „besitzt“, diese Daten zu etwas, das langfristig 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 [27]. „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 Technologieunternehmen würden nichts lieber tun, als Ihre Daten zu besitzen und sie wie Eigentum zu behandeln, welches Sie verkaufen können.“

Werden wir wirklich in unserer Badehose abstimmen?

Im März 2021, kurz nach dem Nein des Schweizer Volkes zum ersten Entwurf des e-ID-Gesetzes, veröffentlichte das Por-

tal Swissinfo (in fünf Sprachen) einen Beitrag von Ian Richards, einem Wirtschaftswissenschaftler der Vereinten Nationen, der sich bereits in der Vergangenheit durch Beiträge hervortat, in denen er die Vorteile des Covid-QR-Codes „trotz aller Kontroversen" hervorhob [28]. Sein Text mit dem Titel „Impfpässe könnten Schweizer Nein zur E-ID obsolet machen" [29] war ähnlich gelagert und stellte eine Utopie vor, in der mit diesem Gerät alles einfach, bequem und reibungslos sein könnte. Für ihn bestand kein Zweifel daran, dass die Schweizer im Sommer 2021 die Vorteile der Covid-19-Zertifikate ausprobieren würden und nicht mehr zurück wollen, im Gegenteil: „Ja, die Impfpässe bleiben umstritten. Die Weltgesundheits-Organisation schreibt: ‚Es gibt immer noch kritische Unbekannte bezüglich der Wirksamkeit der Impfung bei der Reduzierung der Übertragung', und es sei wenig darüber diskutiert worden, wie diese geregelt werden sollten. Aber wenn es darauf ankommt, zwischen einem weiteren Sommer in teuren Bergferienorten oder frisch gegrilltem Fisch in einer Taverne am Strand zu wählen, werden viele wahrscheinlich für die Badehose stimmen, ihren digitalen Impfpass herunterladen und dann ins Ausland reisen. Ferienreisende in anderen Ländern werden das Gleiche tun. Und bei der Rückkehr in die Heimat werden sich die Regierungen wahrscheinlich beeilen, für Pässe und andere Dokumente das zu unternehmen, was die IATA für Impfzeugnisse gemacht hat und was der Irak, Benin und British Columbia tun. In sechs Monaten wird die Hauptkritik an der E-ID vielleicht nicht sein, dass sie zu weit geht, sondern dass sie nicht weit genug geht."

Während in der Schweiz die Vernehmlassung zum neuen e-ID-Gesetz gerade abgeschlossen wurde und der Bundesrat hofft, sich an den Zeitplan der EU für die Annahme dieses Systems auf Ende 2022 halten zu können, wäre es wünschenswert, dass die Bürgerinnen und Bürger die Gelegenheit erhalten, die Auswirkungen und die Verbindung zum Covid-19-Zertifikat gründlich zu überdenken. Denn, wie Elizabeth Renieris im April 2021 festellte, müssen die 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 [30]. „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. Das Covid-19-Zertifikat hat sich jedoch bereits als eine „erweiterbare" Lösung erwiesen [31].

> In der Tat", so die Forscherin, „müssen wir untersuchen, welche Machtverschiebungen und omnipräsente umfassende Identifikation in vielen Lebensbereichen, dieses System bewirken wird".

Auch Tommy Cooke und Benjamin J. Muller sehen eine „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 zukünftigen Iterationen 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.

Tommy Cooke und Benjamin J. 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 verantwort-

Quellen:

[17] Ledger Insights, Ledger Insights „Immunity certificates don't have to give up our data privacy. Here's why.", am 25.05.2020, *<https://www.ledgerinsights.com/immunity-certificates-dont-have-to-give-up-our-data-privacy/>*

[18] Hackernoon „Covid-19 Vaccination Passes Could Cataylze Self-Sovereign Identity Adoption", am 10.06.2021, *<https://hackernoon.com/covid-19-vaccination-passes-could-cataylze-self-sovereign-identity-adoption-6x3m3563>*

[19] Aargauer Zeitung, Othmar von Matt „Kaum einer wollte die E-ID – Covid könnte das nun ändern", am 30.07.2021, *<https://www.aargauer-zeitung.ch/schweiz/kaum-einer-wollte-die-e-id-covid-konnte-das-nun-andern-ld.2168830>*

[20] ICAEW „Blockchain and the future of accountancy", *<https://www.icaew.com/technical/technology/blockchain/blockchain-articles/blockchain-and-the-accounting-perspective>*

[21] CoinGape, Guest Author „How to Take Advantage of a Secure Blockchain Logging?", am 21.02.2019, *<https://coingape.com/how-to-take-advantage-of-a-secure-blockchain-logging/>*

[22] Medium Berkman Klein Center, Elizabeth M. Renieris „Forget erasure: why blockchain is really incompatible with the GDPR", am 23.09.2019, *<https://medium.com/berkman-klein-center/forget-erasure-why-blockchain-is-really-incompatible-with-the-gdpr-9f60374e90f3>*

[23] Ledger Insights, Ledger Insights „Advisor resigns from ID2020 objecting to blockchain immunity passports for COVID-19", am 28.05.2020, *<https://www.ledgerinsights.com/id2020-resignation-blockchain-covid-19-immunity-passports/>*

[24] Linkedin, Paul Oude Luttighuis „Why the blockchain is centralistic", am 11.09.2017, *<https://www.linkedin.com/pulse/why-blockchain-centralistic-paul-oude-luttighuis/>*

[25] Public Books, Natasha Dow Schüll „The Folly of Technological Solutionism: An Interview with Evgeny Morozov", am 09.09.2013, *<https://www.publicbooks.org/the-folly-of-technological-solutionism-an-interview-with-evgeny-morozov/>*

[26] Medium, Elizabeth M. Renieris „Do we really want to "sell" ourselves? The risks of a property law paradigm for personal data ownership.", am 23.09.2018, *<https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa>*

[27] Slate, Elizabeth M. Renieris, Ravi Naik, Jonnie Penn „You Really Don't Want to Sell Your Data", am 07.04.2020, *<https://slate.com/technology/2020/04/sell-your-own-data-bad-idea.html>*

[28] Now And Then News „Vaccine Passports Are Controversial But Their Technology Will Bring Big Benefits to Developing Countries — Global Issues", am 04.03.2021, *<https://nowandthennews.com/2021/03/04/vaccine-passports-are-controversial-but-their-technology-will-bring-big-benefits-to-developing-countries-global-issues/>*

[29] Swissinfo, Ian Richards „Comment les passeports vaccinaux pourraient rendre le refus de l'eID obsolète", am 24.03.2021, *<https://www.swissinfo.ch/fre/comment-les-passeports-vaccinaux-pourraient-rendre-le-refus-de-l-eid-obsolète/46472786>*

[30] Centre for International Governance Innovation, Elizabeth M. Renieris „What's Really at Stake with Vaccine Passports", am 05.04.2021, *<https://www.cigionline.org/articles/whats-really-stake-vaccine-passports/>*

[31] Re-Check, Catherine Riva, Serena Tinari, Jannes van Roermund „«Function creep» im Pandemie-Modus: der seltsame Fall der Covid-19-Zertifikate (2/3)", am 02.01.2022, *<https://free21.org/der-seltsame-fall-der-covid-19-zertifikate-2/>*

[32] *<https://twitter.com/caitoz/sta-*

Autor: Catherine Riva

ist investigative Journalistin und spezialisiert auf den Gesundheitsbereich. (EBM, Methodologie, pharmazeutische Produkte, öffentliche Gesundheit, Regulierung, Interessenkonflikte).

Sie ist Mitbegründerin von Re-Check, Investigating and Mapping Health Affairs und wird regelmäßig von Universitäten und Journalistenorganisationen als Trainerin und Referentin eingeladen.

Sie ist außerdem Übersetzerin und Autorin.

Autor: Serena Tinari

wurde 1972 in Pescara, Italien, geboren und wuchs in Rom auf. Seit 2000 lebt sie in Bern, Schweiz. Zusammen mit Catherine Riva ist sie Mitbegründerin von Re-Check, einer Non-Profit-Organisation für Investigating & Mapping Health Affairs. Seit 1994 als Journalistin tätig; 2002-2015 war sie als investigative Reporterin für den öffentlich-rechtlichen Schweizer Rundfunk tätig: für Falò RSI und Patti chiari (RSI) und für die Rundschau (SRF). Seit 2015 ist sie freiberuflich tätig. Sie ist Mitglied des International Consortium of Investigative Journalists (ICIJ), Präsidentin der Schweizer Organisation für investigativen Journalismus investigativ.ch und Beiratsmitglied von IRPI und journalismfund.eu. Sie unterstützt die Aktivitäten des Global Network for Investigative Journalism (GIJN).

Autor: Jannes van Roermund

ist Journalist. Von Warschau aus arbeitete er als Korrespondent in Mittel- und Osteuropa und veröffentlichte u.a. im Reformatorisch Dagblad, VICE, de Volkskrant, Vrij Nederland und Follow The Money. Heute lebt er wieder in den Niederlanden, wo er als Redakteur bei De Telegraaf arbeitet und Mitbegründer von OverNu ist.

lich 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 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 sich an die von Ian Richards beschriebene „Badehose“- und „reibungslosen“ Fahrplan halten. Oder ob sie im Gegenteil in diesem Gerät eine beunruhigende Entwicklung sehen, weil die bisherige Verwendung des QR-Codes für 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 die Mächtigen wollen das, und das aus gutem Grund.“ [32]

Publiziert auf Free21 am 04.01.2022, 6:00 Uhr