Digital Identity - gigantischer Angriff auf Privatsphäre

Categories : Corona-Virus & Crash, Einleitung "Für immer Frei", Was droht dem Bürger ?

[vc_row][vc_column][vc_column_text]

COVID-19 ist ein gewaltiger "Türöffner" für Digital Identity

Im Ergebnis geht es um die Schaffung einer jederzeit umfassend kontrollierbaren „digitalen Identität“ für jeden Bewohner auf dieser Welt. Alles beginnt in den hochentwickelten Ländern dieser Welt.

Die im Davoser Weltwirtschaftsforum zusammengeschlossenen Großkonzerne arbeiten derzeit zusammen mit dem US-Inlandsgeheimdienst Homeland Security sowie verschiedenen Stiftungen zunächst an der totalen Kontrolle von Flugreisenden.

Im Jahr 2018 bereits wurde das Projekt mit dem Namen

„The Known Traveller Digital Identity-Projekt“

vorgestellt.

Das kann jeder nachlesen H I E R .

Seit 26. März 2020 liegt jetzt auch das “Whitepaper” vor.

Auch das kann jeder nachlesen H I E R .

Beide Dokumente kann man sich als PDF herunterladen und dauerhaft für sich sichern.

Lesen sollen diese Berichte eigentlich nur die am digitalen Überwachungs- und Sicherheitsgeschäft Beteiligten. Diese sprechen aus nachvollziehbaren Gründen lieber von “Digital Identity” als von “digitaler Total-Kontrolle”. Erstellt wurde alles von der Beratungsgesellschaft “Accenture”.

Das Ziel ist, dass alle Reisenden künftig ihre persönlichen Daten an Flughäfen und Einwanderungspunkten angeben müssen wie

- Identitätsnachweis,
- Reisehistorie,
- Bankdaten,
- Hotelübernachtungen,
- Mietwagenbuchungen,
- Dokumente von Ämtern
- und vieles mehr.

Wir befüllen demnach selbst eine Datenbank mit verlässlichen Informationen über uns. Drücken wir es genauer aus: Wir bitten oder ermächtigen andere, in diese Bank Daten über uns einzustellen. Das soll dann so etwas wie ein staatlicher Identitätsnachweis sein.

Wenn wir eine Grenze überschreiten wollen, geben wir den Behörden “freiwillig” Zugang zu unseren Daten, damit sie sich vorab überzeugen können, wie lieb und harmlos wir sind. Mittels Gesichtserkennung und unserem - hoffentlich doch bitte - biometrisch mit uns verknüpften Smartphone, können sie sich beim Grenzübergang davon überzeugen, dass wir wirklich sind, wer wir behaupten zu sein. Wenn wir unterwürfig genug beim digitalen Belege sammeln und freigiebig genug mit diesen Daten waren, dürfen wir zur Belohnung an den Schlangen der anderen Reisenden vorbeigehen, werden bevorzugt behandelt und minimal kontrolliert. Wenn nicht, kann der Grenzbeamte, gestützt auf die übermittelten Informationen,

> *„tiefgehender Fragen stellen, etwa um seine jüngsten Aktivitäten besser zu verstehen“,*

wie es so schön nachzulesen ist in den oben bezeichneten Dokumenten.

Man kann sich leicht ausmalen, wie „freiwillig“ diese Datenfreigabe sein wird, wenn das System einmal etabliert ist. Den Testlauf machen nun die Grenzbehörden von Kanada und den Niederlanden, mit den Fluggesellschaften KLM und Air Canada an den Flughäfen Amsterdam sowie Toronto und Montreal.

Grenzbehörden sind der ideale Katalysator für ein solches System der Überwachung und Datenfreigabe, in das nach und nach alle Regierungen der Welt eingebunden werden sollen. Das läuft dann so ab wie die Einführung des automatischen Informationsaustauschs von Banken (CRS), was sich zwischenzeitlich wie ein Krebsgeschwür in der Welt ausgebreitet hat und nur noch wenige Inseln der Vertraulichkeit übrig gelassen hat. Es ist absehbar: Wenn ein Land nicht mitmacht, können deren Bürger irgendwann nur noch unter großen Schwierigkeiten international reisen.

Wenn das gelungen ist, wenn alle Regierungen sich diesem Standard für den erzwungenen freiwilligen Datenaustausch mit den Bürgern angeschlossen haben, dann dürfen wir unsere Daten auch

> *„für **alltägliche** Anwendungen“*

in Interaktion mit Unternehmen und Behörden hergeben (die Fettung ist dem Originaldokument entnommen).

Es kommt im Ergebnis die Komplettüberwachung auf uns zu. Nach der Luftverkehrs-Testphase wird das auf alle Lebensbereiche der Bürger ausgeweitet werden.

Das Weißbuch macht die große Ambition des Projekts direkt schon in der Einführung deutlich:

> *“Dieses Papier beschreibt den Anspruch von KTDI die Grundlagen für ein global akzeptiertes, dezentralisiertes Identitäts-Ökosystem zu legen. … Der Erfolg wird von der Kooperation zwischen den Regierungen der Welt, Regulierern, Fluggesellschaften, Technologieanbietern und anderen Spielern abhängen, um globale Standards und technische Spezifikationen festzulegen, an die sich alle halten.”*

Die Voraussetzungen, diesen globalen Überwachungsstandard durchzusetzen sind leider hervorragend, nicht zuletzt nach den Überwachungstools, die im Zusammenhnag mit COVID-19 entwickelt werden. Genutzt werden sollen die vom World Wide Web Consortium (W3C) derzeit entwickelten Standards für

“verifiable credentials” (verifizierbare Belege)

und dezentralisierte Identifikatoren.

Zur Erklärung: W3C ist das wichtigste Standardsetzer-Gremium für das Internet und wird von überwiegend US-amerikanischen Internet- und Telekommunikationsfirmen dominiert.

Die Mitglieder von W3C überschneiden sich stark mit denen der

Decentralized Identity Foundation,

die Multis wie Microsoft und viele kleinere Firmen der digitalen Sicherheitsbranche gegründet haben, um die Decentralized Identity Foundation, voranzutreiben.
Die Unternehmen, die sich hier tummeln, haben oft sehr enge Kontakte zu den Geheimdiensten, wenn sie nicht sogar mit dem Geld der Geheimdienste aufgebaut wurden. Die US Homeland Security war von Anfang an am “Know Traveller Projekt” beteiligt. Auf den einschlägigen Digital Identity Foren treffen sich Vertreter dieser Firmen mit allem was in der Welt der Sicherheitsbehörden und Geheimdienste Rang und Namen hat.

Angewendet wird das bestens bekannt Prinzip der reinen Fiktion von Freiwilligkeit. Fast allen Überwachungsansinnen der Webseitenbetreiber muss man zustimmen, wenn man sich im World Wide Web heutzutage bewegen will. Das wird hier kopiert. Das insoweit abgepresste “ausdrückliche Einverständnis zur Datennutzung”, das man jedes mal geben muss, wenn man in diesem künftigen System eine staatliche Leistung erhalten oder nur irgendetwas digital bezahlen will. Es bleibt einem gar keine Alternative, als zuzustimmen.

Besonders perfide an dem System:

> *“Eine ausgebende Behörde kann einen verifizierbaren Beleg, den sie vorher ausgestellt hat, zurückrufen, indem sie den verschlüsselten blockchainbasierten Akkumulator entsprechend aktualisiert.”*

Aldous Huxley war mit seinen Vorstellungen vergleichsweise ein Dilettant.

Bei Digital Identity geht es nicht einfach darum – wie es dem nichtsahnendem Volk gern vorgemacht wird – jedem eine einfache Möglichkeit zu geben, per digitaler Geburtsurkunde oder digitalem Personalausweis nachzuweisen, wer man ist. Es geht darum, alles was über eine Person bekannt ist, in eine von allen teilnehmenden Konzernen und Regierungen anzapfbare und hoheitlich jederzeit manipulierbare Datenbank einzuspeisen.

Angeblich hat das Weltwirtschaftsforum noch kein Konzept für die Governance dieser global-totalitären Kontrollinfrastruktur erstellt, also dafür, wer an den Schaltstellen dieses Systems sitzen soll. Im Weißbuch heißt es:

> *“Die Arbeit an der Definition und Entwicklung eines angemessenen Governance-Rahmens für das KTDI-Konzept geht weiter und wird in einem zukünftigen Bericht thematisiert werden.”*

Die Regierungen sollen also mitmachen, ohne dass klar ist, wer die Fäden in der Hand hält. In Wahrheit ist das natürlich schon klar. Es ist Washington und es sind die großen amerikanischen Konzerne, direkt oder über Gremien wie Weltwirtschaftsforum, W3C, FATF und viele mehr, die sie dominieren.
Trotzdem machen die Regierungen eifrig mit bei diesem von den Konzernen und der US-Homeland Security im Ramen des im Weltwirtschaftsforums entwickelten globalen Überwachungskonzeptes.

Die Regierungen von 21 Ländern, darunter Deutschland, haben bereits knapp drei Monate nach der Tagung des Weltwirtschaftsforum, auf der das Known-Traveller-Konzept präsentiert wurde, eine “European Blockchain Partnership” gebildet, um das Überwachungskonzept des Weltwirtschaftsforums in seiner europäischen Inkarnation eSSIF voranzubringen.

Einen sehr guten Vorgeschmack auf das, was uns blüht, erleben wir derzeit in der Reaktion auf Covid-19 in Südkorea und vor allem im chinesischen Wuhan und dem was bei uns in derselben Richtung angedacht und teilweise getan wird:

Totale algorithmische Bevölkerungskontrolle.

- Wer in Wuhan keinen grünen Button auf seinem Überwachungs-Smartphone vorweisen kann und dergestalt signalisiert, dass er wahrscheinlich nicht infiziert ist, der kann sich höchstens zu Fuß bewegen und darf Restaurants und ähnliches nicht betreten.
- In Südkorea werden Aufnahmen von Überwachungskameras, Kreditkartendaten und GPS-Daten ausgewertet, um potentielle Virusträger zu identifizieren und zu verfolgen.

Covid-19 ist wie ein Himmelsgeschenk für die Pläne des Weltwirtschaftsforums. Dank Covid-19 finden sehr viele Menschen diese totalitären Möglichkeiten jetzt sogar erstrebenswert.

Können wir uns wehren?
In Wirklichkeit nicht!

Aber wir können ausweichen, so weit es geht.

1. Gegen den Automatisierten Informationsaustausch von Bankdaten im Rahmen des CRS kann man Konten einrichten bei Finanzdienstleistern, die da nicht oder noch nicht mitmachen. Man kann und muss schlussendlich einen Steuerwohnsitz begründen in einem besteuerungsfreundlichen Land.
2. Den Freiheitsberaubungen der Digital Identity kann man die Schärfe nehmen, indem man Staatsbürger eines Landes wird, die sich dem internationalen Überwachungssystem zwar auch nicht dauerhaft entziehen wird können, wenn seine Bürger ihre Reisefreiheit behalten sollen. Das aber ist weniger dramatisch, wenn dieses Land die Daten seines Bürgers nicht missbraucht, beispielsweise weil es sehr besteuerungsfreundlich ist und in Wirklichkeit an den Daten gar nicht interessiert ist. Und wenn der Reisepass dieses Landes weitgehend visafreies reisen ermöglicht. Beispiel hier.

ZUM KONTAKTFORMULAR[/vc_column_text][/vc_column][/vc_row]