RUBIKON

Freitag, 10. April 2020, 11:00 Uhr
~10 Minuten Lesezeit

Im Schatten der Pandemie

Die totalitäre Horrorvision des Weltwirtschaftsforums soll Wirklichkeit werden.

von Norbert Häring
Foto: Sjstudio6/Shutterstock.com

Beim jährlichen Milliardärsstelldichein in Davos Anfang 2018 wurde ein im Auftrag des Weltwirtschaftsforums erstelltes Pilotprojekt für die Überwachung von Flugreisenden beschlossen, das ich damals als „totalitäre Horrorvision" vorstellte. Ein nun veröffentlichter Nachfolgebericht zeigt, dass der Club der größten multinationalen Konzerne eifrig und erfolgreich daran arbeitet, die Regierungen und die EU in die Umsetzung dieser Horrorvision einzuspannen.

Das Projekt läuft bisher unter dem Titel „Der bekannte Reisende", im Original „The Known Traveller Digital Identity-Projekt", kurz KTDI.

Wie der damalige Bericht ist Ende Januar auch der Nachfolgebericht, das **KTDI White Paper** (https://www.weforum.org/reports/the-known-traveller-unlocking-the-potential-of-digital-identity-for-secure-and-seamless-travel), ohne jede Fanfare im Internet veröffentlicht worden. Lesen sollen diese von der Beratungsgesellschaft *Accenture* erstellten Berichte nur die am digitalen Überwachungs- und Sicherheitsgeschäft Beteiligten. Diese sprechen aus nachvollziehbaren Gründen lieber von Digital Identity als von digitaler Kontrolle.

So soll es ablaufen: Wir befüllen selbst eine Datenbank mit verlässlichen Informationen über uns, genauer, wir bitten oder ermächtigen andere, dort Daten über uns einzustellen. Das soll zuvorderst ein staatlicher Identitätsnachweis sein, aber auch unsere Reisehistorie, Bankdaten, Hotelübernachtungen, Mietwagenbuchungen, Dokumente von Universitäten, Ämtern und sehr vieles mehr. Wenn wir eine Grenze überschreiten wollen, geben wir den Behörden freiwillig Zugang zu diesen Daten, damit sie sich vorab überzeugen können, dass wir harmlos sind. Mittels Gesichtserkennung und unserem (idealerweise) biometrisch mit uns verknüpften Smartphone, können sie sich beim Grenzübergang davon überzeugen, dass wir sind, wer wir behaupten zu sein.

Wenn wir fleißig genug beim Sammeln digitaler Belege 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 sich allerdings Zweifel an den Absichten eines Reisenden auftun, kann der Grenzbeamte ihm, gestützt auf die übermittelten Informationen,

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

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

Konzerne wie *Visa* und *Google* sind natürlich nicht aus reinem weltbürgerlichen Pflichtgefühl so engagiert, um für die Polizeibehörden auf eigene Kosten ein solches System auszuarbeiten. Vielmehr sind die Grenzbehörden erklärtermaßen der ideale Katalysator, um die kritische Masse für ein solches System der Selbstüberwachung und Datenfreigabe zu schaffen und dabei nach und nach alle Regierungen der Welt einzubinden. Denn wenn eine nicht mitmacht, können deren Bürger irgendwann nur noch unter großen Schwierigkeiten international reisen.

So heißt es im ersten Bericht, ebenso wie im jetzigen Weißbuch, dass die Selbstüberwachung an der Grenze nur dazu diene, eine kritische Anfangsmasse an Beteiligten an dem globalen Standard zu schaffen, den man so einführen will. 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 (Fettung im Original). Genannt werden in beiden Berichten vor allem Gesundheit, Bildung und Erziehung, Bankwesen, humanitäre Hilfe und Wahlen.

Ein globales, totalitäres System

Das KTDI-Weißbuch macht die große Ambition des Projekts 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 hervorragend. Genutzt werden sollen die vom *World Wide Web Consortium* (W3C) derzeit entwickelten Standards für „verifiable credentials” (verifizierbare Belege) und dezentralisierte Identifikatoren. 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** (https://medium.com/decentralized-identity/decentralized-identity-foundation-grows-to-56-members-in-our-first-year-3ec117e811d8), die Multis wie *Microsoft* und viele kleinere Firmen der digitalen Sicherheitsbranche gegründet haben, um die globalen Identitätskontroll-Standards 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 Beginn an dem *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.

> ***Der Trick ist die Fiktion von Freiwilligkeit, das abgepresste aber ausdrückliche Einverständnis zur Datennutzung, das man jedes Mal geben muss, wenn man in diesem System eine staatliche Leistung erhalten oder nur irgendetwas digital bezahlen will.***

So wie man jetzt schon fast allen Überwachungsansinnen der Webseitenbetreiber zustimmen muss, wenn man sich im World Wide Web bewegen will.

Besonders perfide an dem System:

„*Eine ausgebende Behörde kann einen verifizierbaren Beleg, den sie vorher ausgestellt hat, zurückrufen, indem sie den verschlüsselten Blockchain-basierten Akkumulator entsprechend aktualisiert.*“

Stellen wir uns das einmal vor, wie es aussieht, wenn dieses System wie beabsichtigt in der ganzen Welt umgesetzt ist, in jedem noch so repressiven Land. Nehmen wir dabei an, dass die parallel vorangetriebene Bargeldabschaffung erfolgreich abgeschlossen ist. Für alles, was man tun will, ist man darauf angewiesen, dass in der Datenbank an den richtigen Stellen ein Häkchen steht. Fällt man bei der eigenen Regierung in Ungnade, zieht sie das Häkchen beim Personalausweis nachträglich zurück.

Man kann dann versuchen, es noch eine Weile durchzuhalten. Am besten aber macht man es so, wie im Science-Fiction-Film „Sonne auf Kredit” von Michel Grimaud aus dem Jahr 1975. Wenn die elektronische Karte, die man in der Romanzukunft überall braucht, um sich zu bewegen und seine Rationen zu bekommen, von einem der Kontrollautomaten eingezogen wird, geht man „freiwillig” ins Gefängnis und bleibt dort, weil man sonst verhungert.

Auch wenn die US-Regierung oder die von ihren Geheimdiensten kontrollierten Algorithmen irgendjemanden auf der Welt auf dem

Kieker haben, können sie entsprechendes bewirken. Entweder sie bringen die jeweilige Regierung dazu, alle digitalen Dokumente der Zielperson ungültig zu machen, oder die US-Digitalkonzerne, die das System kontrollieren, tun das, oder die privaten US-Kreditwürdigkeitsbescheiniger setzen die Kreditwürdigkeit auf Null.

Vieles davon geht jetzt schon. Aber erst wenn es einen global akzeptierten technischen Standard gibt, mit dem man auf alle diese Daten und Dokumente zugreifen kann, ist das System umfassend und perfekt. Erst dann können Washington beziehungsweise *Fort Meade* und *Langley* vom heimischen Computer aus alle in jedem teilnehmenden Winkel der Erde kontrollieren — und nationale autoritäre Regierungen können alle im eigenen Einflussgebiet kontrollieren, egal ob sie sich im Inland oder Ausland aufhalten.

Minority Report lässt grüßen

Vielleicht bekommt man den Nasenring sogar dann unsanft zu spüren, wenn man gar nichts getan hat, nur weil ein Rechenmodell zu dem Schluss kommt, man könnte demnächst Ärger machen, so wie im Film „Minority Report". Die Ambition dazu ist im ersten KTDI-Bericht des Weltwirtschaftsforums in Form eines graphisch hervorgehobenen Zitats des *Google*-Managers Rob Torres dokumentiert:

„*Technologieunternehmen haben große Fortschritte beim Data-Mining, Maschinenlernen und künstlicher Intelligenz gemacht, die fortgeschrittene prognostische Analysen ermöglichen. In Kombination mit von den Passagieren gelieferten Informationen können diese Technologien von Regierungen genutzt werden, um (…) komplexe Muster in großen Datenbeständen mit dem Ziel zu analysieren, Sicherheitsrisiken an Grenzen vorherzusagen.*"

Das Zitat macht deutlich, dass es bei Digital Identity nicht einfach darum geht — wie es dem dummen Volk gern vorgemacht wird — jedem eine einfache Möglichkeit zu geben, per digitaler Geburtsurkunde oder digitalem Personalausweis nachzuweisen, wer man ist. Wir werden weiter unten noch auf ein weiteres Zitat aus anderer Quelle stoßen, welches das belegt.

> ***Nein, 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.***

Damit die Unternehmen uns als Konsumvieh jeweils in die richtige Box lenken und dort optimal abkassieren können, und uns als Arbeitstiere billig halten und kontrollieren können. Und damit die Regierungen alle gewaltfrei an einem normalerweise unmerklichen Nasenring führen und am Ausbrechen aus dem System hindern können.

Bemerkenswerter Weise hat das Weltwirtschaftsforum angeblich 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 sich also diesem Konzept verschreiben, ohne dass klar ist, wer die Fäden in der Hand hält. In Wahrheit ist das natürlich schon klar. Es ist Washington und die großen amerikanischen Konzerne, direkt oder über Gremien wie Weltwirtschaftsforum, W3C, FATF und viele mehr, die sie dominieren.

Die Regierungen machen willfährig mit

Trotzdem machen die Regierungen eifrig mit bei diesem von den Konzernen und der US-*Homeland Security* im Weltwirtschaftsforum entwickelten globalen Überwachungskonzept. Es wird von den teilnehmenden Unternehmen der Sicherheits- und Identitätsbranche unter dem schönfärberischen Namen *Self-Sovereign Identity* (SSI) vermarktet. In Deutschland trommelt die Regierung seit gut zwei Jahren unterwürfig unter dem Namen Dateneigentum für diesen feuchten Traum der Datenkraken und Überwachungsbehörden.

In Brüssel fängt das Kürzel SSI an sich durchzusetzen. Das EU-Nebenorgan Europäischer Wirtschafts- und Sozialausschuss, in dem Arbeitgeberverbände, Gewerkschaften und andere Interessengruppen vertreten sind und die „organisierte Bürgergesellschaft" repräsentieren sollen, hat ein ***European Self-Sovereign Identity Framework* (eSSIF)** (https://www.eesc.europa.eu/en/news-media/presentations/european-self-sovereign-identity-framework) entwickelt, oder — vermutlich besser ausgedrückt — sich vom Weltwirtschaftsforum unterschieben lassen. Es ist praktisch eins zu eins das Horrorkonzept des Weltwirtschaftsforums. Man findet genau die gleichen Grafiken darin und so schöne Sätze wie:

> ***„Wenn wir digitale Identität sagen, müssen wir es verstehen als die Summe aller Attribute, die über uns in der digitalen Welt existieren, eine laufend wachsende und sich entwickelnde Sammlung von Datenpunkten."***

Das Zitat ist übernommen aus dem „**EU blockchain observatory report on digital identity and blockchain** (https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf)". Digitale Identität meint also alles, was es über

uns, unser Tun und unsere Vorlieben zu wissen gibt.

Die Regierungen von 21 Ländern, darunter Deutschland, haben bereits knapp drei Monate nach der Tagung des Weltwirtschaftsforums, auf der das Known-Traveller-Konzept präsentiert wurde, eine „**European Blockchain Partnership** (https://blockchainwelt.de/european-blockchain-partnership-ebp-steigendes-interesse-an-distributed-ledger-technologie/)“ gebildet, um das Überwachungskonzept des Weltwirtschaftsforums in seiner europäischen Inkarnation eSSIF voranzubringen. Dabei ist als ein letztes Arbeitsziel dieser Partnerschaft in der oben verlinkten Präsentation des Wirtschafts- und Sozialausschusses aufgeführt, dass es auch darum gehen soll, herauszufinden, wie man bei der Umsetzung von SSID europäische demokratische Werte bewahren kann. Viel Erfolg, das wird schwer!

Es gibt noch einige mehr Gruppen und Partnerschaften auf europäischer Ebene zur Umsetzung von SSID, die alle hier aufzuführen den Rahmen sprengen würde. Klar sollte geworden sein: Bei KTDI und SSID geht es nicht um unrealistische Idealvorstellungen Washingtons und der Datenkraken, sondern um etwas, was weltweit mit sehr viel Engagement und großen Erfolgsaussichten im Hintergrund vorangetrieben wird. Wir werden wenig davon mitbekommen, bis es da ist.

Covid-19 bringt den Vorgeschmack

Einen sehr guten Vorgeschmack auf das, was uns nach den Vorstellungen der Konzerne und Regierungen 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, der signalisiert, dass man wahrscheinlich nicht infiziert ist, der kann sich höchstens zu Fuß bewegen und darf Restaurants und ähnliches nicht betreten. In **Südkorea** (https://www.datenschutz-notizen.de/should-we-copy-the-south-korean-model-of-fighting-covid-19-4725408/) 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.

Wenn das KTDI-Konzept einmal umgesetzt und zu SSID verallgemeinert eingeführt ist, brauchen die Aufseher in solchen Fällen nur noch einen Häkchen in der Datenbank zu setzen, ob man getestet wurde, oder ob die eigenen GPS-Daten in unmittelbarer Nähe eines Infizierten oder in einem Risikogebiet registriert wurden, und schon kann die Bewegungs- und Handlungsfreiheit beliebig und automatisiert eingeschränkt werden. Und dank Covid-19 finden sehr viele Menschen diese totalitären Möglichkeiten jetzt sogar erstrebenswert.

Norbert Häring, Jahrgang 1963, ist Wirtschaftsjournalist, promovierter Volkswirt, **Blogger** (http://norberthaering.de) und preisgekrönter Autor mehrerer populärer Wirtschaftsbücher. Zuletzt erschien von ihm „**Schönes neues Geld: PayPal, WeChat, Amazon Go — Uns droht eine totalitäre Weltwährung** (https://www.campus.de/buecher-campus-verlag/wirtschaft-gesellschaft/wirtschaft/schoenes_neues_geld-

15082.html)“.