Quelle: Unsplash

Echte Informationelle Selbstbestimmung beginnt mit einer souveränen digitalen Identität

Analyse und Vorschlag für eine dezentrale Identitäts Architektur

Blogpost auf omnisophie.com

Gunter Dueck, Max Senges[1], Martin Schössler[2]

Übersicht

[1] Max Senges, Gastforscher beim Stanford Center for Democracy, Development and the Rule of Law. Max arbeitet bei Google, dieser Post ist aber in seiner akademischen Rolle geschrieben und spiegelt nicht die Positionen seines Arbeitgebers wieder. Mehr unter maxsenges.com

[2] Martin Schössler ist Managing Partner bei der auf Wachstumsstrategien spezialisierten Beratungsfirma CAUSA sowie Teilhaber an jungen Unternehmen. Zuvor war er bei „The Economist“ in London und Frankfurt tätig.

Mein Identitätscockpit

In der analogen und der digitalen Welt hinterlassen haben wir einen „Data Footprint“ oder einen Identitätsabdruck; wir sind dokumentiert, authentifiziert, tragen Kundennummern, geben öffentliche Likes ab und sorgen uns um unsere Scores bei Banken und der Polizei. Wir haben längst den Überblick verloren. In diesem Beitrag wollen wir uns Gedanken machen, wie man die entstandene Komplexität wieder zurückführt. Dazu schlagen wir ein Identitätscockpit[3] vor. Die Bezeichnung „Cockpit“ wird gerade von der deutschen Regierung für ein geplantes Konzept verwendet, das Bürgern die Kontrolle über die bei verschiedensten staatlichen Stellen gespeicherten Daten geben soll. Dieses Konzept begradigt vielleicht unser Datenverhältnis zum Staat, greift aber damit ganz sicher zu kurz. Wir wollen eine Diskussion über ein Gesamtkonzept anregen.

- Wir sollten unsere Daten zu größtem Nutzen digital „zusammenhaben“, die Kontrolle über sie wahrnehmen können und wissen, wer über uns wieviel weiß.
- Unsere Daten sollten „gut aufgehoben“ sein, also gesichert und sicher.
- Über allem sollten wir die Prinzipien eines Digital-Humanismus liegen haben – danach dienen die Daten den Menschen und empowern sie selbst, anstatt vorrangig für wirtschaftliche, staatliche und überwachende Zwecke nützlich zu sein

Das Problem – Wir sind zu viele

Wer bin ich ohne meine Daten? Ich stelle mir vor, ich verliere auf einer Auslandsreise in einem fernen Land die Verbindung zu meiner Reisegruppe – und plötzlich sieht man mir an, dass ich hilflos bin. Prompt bin ich Geld, Smartphone und Papiere los. Wer bin ich jetzt, so ganz allein, ohne meine „Identität“? Wer sich tief in diese Situation einfühlt, merkt, wie sehr unsere Identität durch unsere Ausweise aller Art nicht nur definiert, sondern auch dokumentiert und vertrauenswürdig gesichert ist. Es gibt Länder, in die Menschen ganz ohne solche Dokumente leben.
In solchen Ländern bebauen oft arme Familien mühsam ein Stück Land. Da kommt plötzlich jemand mit einem Auto vorbeigefahren und behauptet, ihm gehöre das Land. Ja, gute Frage, wem gehört das Land, wenn es dort keine Grundbücher gibt?
Ahnenforscher beklagen, dass nur Bauern und Adlige aus unserer Vergangenheit gut bekannt seien, weil Grundbücher und Adelsregister allezeit gut geführt wurden, eben, weil konkrete Rechte daran hingen. Mit einigem Glück findet man Menschen noch in Kirchenbüchern. Der Rest ist geschichtlich gesehen vergessen und verloren, denn damals hatten die Menschen keine allgemein dokumentierte Identität.

Was geschieht, wenn unser Haus abbrennt? Wir haben unser Abiturzeugnis und eine Masterurkunde daheim. Ließen sich dafür Ersatzdokumente anfordern? Wo? Auch nach vielen Jahren noch? Oh, meine Fahrzeugpapiere sind auch verbrannt. Gehört mir mein Auto dann noch?

[3] https://www.sueddeutsche.de/politik/behoerden-cockpit-fuer-buergerdaten-1.4632366

Wer seine Rente beantragt, wird nach verlässlichen Nachweisen früherer Praktika gefragt, er muss beweisen, wo er seine Lehre absolviert hat bzw. wie viele Semester er studiert hat, wann und wo er seinen Ersatzdienst ableistete und ob er irgendwo je Unterstützungszahlungen aus Versicherungen bekam. Hilfe! Da fragen wir schon Ergrauten uns: Wer war ich?

Noch schlimmer – wir fragen uns besorgt wie Richard David Precht: Wer bin ich, und wenn ja, wie viele? Sehr viele. Wir sind jemand auf unserer Geburtsurkunde, bei unserer Sozialversicherung, beim Finanzamt, beim Einwohnermeldeamt, bei einigen Banken und Versicherungen, beim Abwasseramt und in Flensburg – und wir sind derjenige auf unseren Kreditkarten, wir haben eine ID bei PayPal, der Deutschlandcard und bei WhatsApp. Ja, wir haben auch eine dürftige Gesundheitskarte ohne viele Daten darauf, einen Organspendeausweis oder auch nicht, einen schlecht geführten Impfpass, und wir haben bei jedem Arzt eine andere Identität: der Augenarzt kennt nur unseren Kopf, der Urologe interessiert sich nicht dafür. Wenn wir verunfallen, kennt man meist weder unsere Blutgruppe noch unsere Allergien. Wer plötzlich schlaganfällig unrettbar nur noch am Tropf überleben kann, wird gegen den eigenen Willen am Leben erhalten, weil man nicht wusste, wo Testament und Patientenverfügungen lagen, als der Notarzt kam.
Wollen Sie in die USA fliegen und ein ESTA-Formular ausfüllen? Man fragt: „Name und Vorname genau wie im Pass“. Wo aber steht der Name im Pass? Im Textteil stehen alle drei Vornamen und der Doktortitel, unten im maschinenlesbaren Teil nur der Rufname und der Nachname. Wer sind wir denn nun im Sinne der USA? Was füllen bloß Spanier mit ihren meist zwei Nachnamen aus?

Wir hoffen Sie stimmen uns zu:

- Wir haben zu viele Identitäten, die wir insgesamt nicht einmal selbst genau kennen.
- Wir werden überall irgendwie anders gesehen – und oft „passen die Identitäten nicht genau zusammen“.
- Wir haben keinen Überblick mehr. Das war früher kein wahrgenommenes Problem; es rückt nun aber in den Fokus, weil alles im Digitalen, rund um das Internet „zusammenkommt“.

Unser Netzbild und das Prinzip des Digitalen Humanismus

Wie nehmen wir darauf Einfluss? Was soll oder darf jeder über uns wissen? So wie wir schon immer wählen konnten, ob wir mit einem Eintrag im Telefonbuch erscheinen oder nicht, so müssten wir selbst Einfluss darüber haben, was von uns für andere sichtbar ist. Können wir Daten über uns löschen lassen? Was sollte sinnvollerweise im Netz über uns zu erfahren sein?

Unser Netzbild - der Datenkörper, den wir durch die Gesamtheit unserer Aktivitäten im Netz schaffen - sollte nicht zu zersplittert sein und zufällig wirken. So, wie wir Selbst- und Fremdbild zusammenhalten sollten, müssen wir wohl auch aktiv mit unserem Netzbild umgehen. Aber wie? Wir müssen uns wohl auf ein grundsätzliches ethisches Prinzip gründen, wie wir mit uns und unseren Datenabbildern umgehen wollen. Solch ein Prinzip gehört ins Zentrum, es soll ins Zentrum und uns leiten - das wäre schon etwas (womit natürlich nicht alles “Böse” gleich abgeschafft wäre). Schopenhauer wird ja so gerne zitiert: Neminem laede; imo omnes, quantum potes, juva [Verletze niemanden; im Gegenteil, hilf allen, soweit du nur kannst]. Prinzipien solcher Art sollten uns leiten! Etwa: *Verletze niemanden; trage konstruktiv zur Weiterentwicklung der digitalen Allmende und zur Entwicklung anderer bei, soweit du nur kannst.*
Ja, so sollen sich unsere Absichten leiten lassen. Und genau das meinen wir, wenn wir vom Digitalen Humanismus sprechen.
In der Psychologie kennen wir den Unterschied zwischen Selbstbild und Fremdbild, die sich bei manchen Menschen ärgerlich und dann zu deren Schaden unterscheiden. Zum Beispiel halten sich überragend viele Menschen für die besseren Autofahrer und man sagt, dass die Intelligenz die einzige Ressource auf der Welt ist, die gerecht verteilt ist; denn jeder findet selbst, dass er reichlich damit gesegnet sei. Ein großes Ziel der Persönlichkeitsentwicklung ist es, Selbst- und Fremdbild in Einklang zu bringen.
Nun kommt noch das Netzbild hinzu. Wenn wir Ego-Googeln, also nach uns selbst surfen, finden wir alle möglichen Bruchstücke über uns, oft völlig Verdrehtes, vieles aus dem Zusammenhang Gerissene oder auch eventuell gar nichts (ist das gut oder schlecht?). Nutzer der sozialen Medien hinterlassen tausende Tweets und Likes. Datenanalysten solcher Netzspuren können daraus ein Netzbild von uns anfertigen, das unsere Persönlichkeit oft besser charakterisiert, als es unser nur meist nur widerwillig eingeweihte Psychotherapeut je könnte.

Hier baut sich ein großes Spannungsfeld auf. Die Werbe-Profis versuchen, über die Kenntnis unseres Netzbildes an unser Portemonnaie zu kommen. Personalabteilungen recherchieren auch in den privaten Posts von Bewerbern oder Mitarbeitern. Kreditgeber schauen sich vielleicht bei digitalen Kartendiensten das Luftbild unseres Anwesens an. Wie viel ist das Haus wert? Wirkt es gepflegt? Züchten Sie Löwenzahn? Geheimdienste und Agitatoren aller Art kämmen unser Netzbild auf Irregularitäten durch. Führen wir etwas im Schilde? Haben wir jemanden beleidigt? Wahlbeeinflusser schicken uns je nach Netzbild-Charakter „Informationen“, mit denen wir gelenkt werden sollen. Auf der anderen Seite staunen wir über Instagram-Stars, professionelle YouTuber und Influencer, die mit einem sorgsam aufgebauten und gepflegten Netzbild zum Teil große Geschäfte machen oder es zur Berühmtheit bringen.

Wollen wir ein Netzbild haben? Wenn ja, welches?

Zum Anfang ein Identitätscockpit

Wir müssen irgendwo konkret anfangen, wenn wir uns nicht in Diskussionen verlieren wollen, welche Ethik idealer als andere sein mag.
Beginnen wir, Datensätze aufzuzählen, die wir im Leben brauchen. Die sollten einfach auf einer Identitätskarte oder gleich in der Cloud gespeichert sein.

- Meine Pässe, (Geburts- etc.) Urkunden und Personaldaten, Adresse, Eltern, Kinder
- Meine unveränderliche Biologie: Fingerabdruck, Augenfarbe, Blutgruppe...
- Mein derzeitiger Gesundheitsstatus: Letzte Untersuchungsdaten, Röntgenbilder
- Meine Urkunden: Führerscheinklassen, Zeugnisse, Arbeitsbescheinigungen, Versicherungen, Hypotheken, Besitzurkunden
- Meine Akten beim Notar: Patientenverfügungen, Erbangelegenheiten, Betreuungsangelegenheiten
- Meine Finanzen: Konten, Karten, Versicherungen und Kredite
- Meine Daten bei Behörden: Einwohnermeldeamt, Finanzamt, Steuernummern, Verkehrssündereinträge, Strafregister
- Meine Konten und Passwörter bei Internetfirmen und bei ihnen freigegebene Daten (Versandadresse, Mailadresse, Alter bei Alkoholkauf, etc)
- Meine Ehrenämter und „Partizipation“
- Meine Veröffentlichungen
- Meine Patente

Solche Daten und noch viel mehr sollten wir sammeln und in einem Cockpit verwalten können. Es muss geregelt werden, wer welche Daten dort eingetragen hat oder eintragen darf. Sie kennen das etwa von Twitter: Dort haben wichtige Personen ein blaues Häkchen; das bedeutet, sie sind wirklich „derjenige“, zum Beispiel „the real Donald Trump“, sonst kann man sich nicht sicher sein, ob da nicht doch ein Comedian unter falschem Namen twittert. In diesem Sinne gibt es in meinem Cockpit Daten, die ich selbst eintragen kann (ohne blaues Häkchen) und solche, die als echte Dokumente von dazu Berechtigten eingefügt wurden. Ich möchte einen blauen Haken von der Uni hinter meiner Doktorurkunde, einen vom Patentamt bei den Patenten, einen vom Arzt bei der Blutgruppe. Es gibt also „meine“ Einträge und „beglaubigte“. Bei Unfällen fragen Ärzte oft nach der Blutgruppe oder nach der letzten Tetanusimpfung. Die mündlichen Antworten der Verunfallten sind für sie eine gewisse Indikation, aber sie dürfen sich eigentlich nicht total auf sie verlassen, sonst hat es schlimme Folgen. Wenn sie dagegen in meinem Cockpit eine notarielle Patientenverfügung sehen, müssen sie entsprechend handeln.
In der Politik wird oft davon geträumt, dass es mehr Bürgerpartizipation gegen sollte. Bitte, übernehmen Sie Ehrenämter! Es könnte doch gut und sinnvoll sein, die Ehrenämter und gemeinnützigen Aktivitäten mit blauem Häkchen in meinem Cockpit einzutragen, dann kann ich darauf öffentlichen Stolz zeigen, indem ich diesen Eintrag als “Ordensersatz” in einem Ehrenamt-Register zu publizieren erlaube.

Alle die Daten sind erstmal nur meine. Ich kann sie dem Arzt freigeben, temporär und für immer. Ich kann das Amt des Schriftführers im lokalen Pokémon-Club aus Angst vor vielsagendem Lächeln für die Öffentlichkeit sperren. Ich kann bei der Firma, von der ich eine Betriebsrente beziehe, den Eintrag „lebt noch / ist tot“ einsehen lassen. Bisher muss jeder eine jährliche Lebensbescheinigung beibringen - beglaubigt vom Amt!

In meinem Cockpit bestimme ich dann selbst, welche Daten ich wem freigebe, für wie lange und für welchen Zweck („Versandadresse nur für heute“). Ich kann Daten für andere sperren oder (wo sinnvoll) ganz löschen.
Für den Internethandel stelle ich mir vor, dass ich in meinem Cockpit Datensätze zusammenstelle, die ich per Link dem Händler bei einer Kontoeröffnung zu nutzen erlaube (Adresse, Kreditkarte etc.). Ich müsste den Händler verpflichten können, diese Daten zu löschen, wenn ich ihm die Nutzung des Datensatzes entziehe. In meinem Cockpit hätte ich am liebsten in dieser Weise alle Portale, bei denen ich angemeldet bin, auf einen Blick...
Ja, und natürlich bekomme ich sofort Bauchgrimmen, wenn ich mir vorstelle, mein Cockpit würde gehackt. Aber das hatte ich damals bei meiner Bankverbindung auch. Gute Frage: Ist etwas sicher, wenn nur lange nichts passiert ist? Wenn wir uns in ersten Ansätzen eine digitale Identität zulegen, darf sie natürlich nicht gestohlen werden können. Wir brauchen sichere IT und harte Gesetze!

Vieles von dem, was wir hier vorstellen, ist anderswo schon verwirklicht. Es gibt zum Beispiel anderswo einheitliche Bürgernummern am ersten Lebenstag, an die man sofort Geburtsurkunde, Blutgruppe und eine erste Mailadresse hängen könnte. Warum haben wir solche Identifikationsnummern nur beim Finanzamt? Warum werden wir von Facebook nicht verpflichtet, bei einer Registrierung gleich unsere Identitätsnummer anzugeben, damit vollkommen klar ist, dass ich selbst es war, der gehetzt hat, wenn ich gehetzt habe?[4] Wenn ich dann im Netz mit anderen Identitäten diskutiere, schaue ich per ID-Nummer dem jeweils anderen digital in die Augen, und ich pralle nicht an seiner digitale Maske ab...

Na, jedenfalls wünschen wir uns das so. Wir wissen, dass es ein bisschen traumtänzerisch ist, denn die Daten müssen zusammengeführt werden, die Behörden, Notare, Ärzte und Pokémon-Clubs müssen amtlich eintragsberechtigt mit blauem Häkchen sein. Wir stehen vor sicherheitstechnischen Herausforderungen, die aber in ersten Staaten - z.B. Estland - schon überwunden wurden. Lassen Sie uns in diesem Sinne nicht große Listen von Wenns und Abers auflisten und wie Schutzschilde verwenden. Lassen Sie uns nicht nur schöne Namen wie Gaia-X für eine europäische Cloud erfinden.

Gehen wir los.

Digitale Identität als fehlendes Element der Internet Architektur?

Aus vielen guten Gründen haben die Väter des Internet vor rund 50 Jahren digitales Identitätsmanagement nicht in die Architektur unseres Informationssystems eingebettet. In den darauffolgenden Dekaden fast ungebremsten Wachstums von Internetinhalten und dessen

[4] Die Anonyme Nutzung von vielen Diensten ist aus verschiedenen Gründen - vor allem aus Angst vor politischer Verfolgung durchaus legitim, aber für diese Nutzung sollte es Sonderregeln oder Bereiche geben.

Verknüpfung mit neuen Diensten hat vor allem die Entwicklung sozialer Medien zur milliardenfachen Abbildung sozialer Beziehungen geführt. Damit wurde die Einführung eines "identity layer" als weitere Protokollschicht für das Internet immer notwendiger.[5]

In der heutigen Welt, in der wir fast alle kontinuierlich online sind, hat das Fehlen eines gemeinsamen, offenen Standards für Identitätsmanagement unter anderem dazu geführt, dass wir als "digital gespaltene Persönlichkeit" bei x verschiedenen Online-Diensten Konten anlegen und damit "ID multihoming" betreiben müssen. Die Unbequemlichkeit, sich x Passwörter merken zu müssen, führte dann zum Erfolg von so genannten Single Sign-On Lösungen.[6] Zukünftig wird Interaktion im digitalen Raum ein noch viel umfassender Teil der persönlichen Identität sein. Wir müssen daher bereits heute den Blick auf die Zukunft weiter fassen, als es die Partikulardiskussionen über Login-Varianten oder einzelne KI-Features zulassen.

Identität kann Teil von Zugangs- oder Kontroll-Technologie sein

Larry Lessig unterscheidet zwischen Technologie-Architekturen, die systemische und meist zentral "Kontrolle" verbessern (Technologies of Control) und Architekturen, bei denen das Technologie-Design so angelegt ist, dass sie Zugang zu politischer Teilhabe, zu wirtschaftlichen Möglichkeiten und deren rechtlicher Absicherung (Kredite, Unternehmensgründung, Landbesitzurkunden, etc.), sowie den Zugang zu Wissen und Bildung erweitert (Technologies of Access).

Das chinesische Social Scoring System ist ein gutes Beispiel für eine Architektur, die vor allem auf Kontrolle ausgerichtet ist: Die Bürger werden in immer weiter greifender Art in ihren Handlungen beobachtet und speziell beim Befolgen von gesellschaftlichen bzw. politischen Normen bewertet. Problematisch ist weiter, dass dafür ein intransparentes und nicht anfechtbares, auf Algorithmen aufbauendes System genutzt wird. Auf Basis dieser Bewertung wird ein Score erstellt, diesem entsprechend erfolgen dann Belohnungen (Anreize) oder Bestrafung (Ausschluss von Privilegien oder Zugang zu Bildung und Arbeitsoptionen).

Der chilenische Ökonom Hernando de Soto beschrieb ein Beispiel für Identität als Zugangs- oder Ermächtigungs-Technologie. Bereits in den 80er Jahren begann die chilenische Regierung (damals noch analoge) Identitäten für meist indigene Bewohner von Favelas zu erstellen und daraufhin Landbesitzurkunden auszugeben. Das Wissen (Rechtssicherheit), dass das Land, auf dem die Favela-Hütten standen, nicht einfach weggenommen werden konnte, führte dazu, dass

---

[5] Für eine Übersicht der Protokollschichten vgl. u.a. https://en.m.wikipedia.org/wiki/World_Wide_Web#/media/File%3AInternet_Key_Layers.png

[6] "(...) Single Sign-On (SSO) ist eine Eigenschaft der Zugriffskontrolle mehrerer verwandter, jedoch unabhängiger Softwaresysteme. Mit dieser Eigenschaft meldet sich ein Benutzer mit einer einzelnen ID und einem Kennwort an, um Zugriff auf ein verbundenes System oder verbundene Systeme zu erhalten, ohne andere Benutzernamen oder Kennwörter zu verwenden, oder in einigen Konfigurationen, um sich nahtlos bei jedem System anzumelden. Im Jahr 2018 belief sich der weltweite Single-Sign-On-Markt auf 770 Millionen US-Dollar, und es wird erwartet, dass er bis Ende 2025 2130 Millionen US-Dollar erreichen wird." Quelle: Reuters, https://www.reuters.com/brandfeatures/venture-capital/article?id=117894

die Bewohner langfristiger dachten und investierten. Dadurch entwickelten sich diese gesellschaftlichen und wirtschaftlichen “Grauzonen” in “normale” Mittelstandsviertel.

Bereits zu einem früheren Zeitpunkt hat David Riesman in seinem Klassiker “Die einsame Masse” aufgezeigt, wie der Wertekompass der westlichen Wert aufgeladen ist und unter den Bedingungen der modernen Massengesellschaft die Basis für die individuelle und gemeinschaftliche Identitätsbestimmung bilden kann. Die Diskussion wird also immer wieder durch ein Wechselspiel von sowohl gesellschaftlichen wie auch technologischen Entwicklungen vorangetrieben. In dem Maße, wie neue Technologien erweiterte Fähigkeiten sowohl für staatliche wie auch nichtstaatliche Akteure ermöglichen, folgt in kurzem Zeitabstand die öffentliche Debatte über die richtige Aneignung. Dies gilt auch für die Frage nach der digitalen Identität, die heute in besonderem Maße mit der Frage nach den Möglichkeiten eines digitalen Humanismus (Rümelin 2018) verknüpft ist.[7]

Daher wollen wir die Diskussion um die Entwicklung einer Digitalen Identitäts-Architektur dahingehend unterstützen, das die informationelle Selbstbestimmung verbessert wird und somit zu einer aufgeklärten, souveränen Gestaltung unserer (digitalen) Lebensweise beiträgt.

Unser Vorschlag ermöglicht eine dezentrale Identitäts-Architektur

Basierend auf einem digital-humanistischen Menschenbild wollen wir im Folgenden einen konkreten Anstoß zur Weiterentwicklung der bestehenden Lösungen hin zu einer universellen digitalen Identitätsarchitektur (kurz DIA) machen.

Informationstechnologie ist heute beinahe unauflöslich mit der Lebensführung und dem Entscheidungsverhalten der Bürger verknüpft und ihre Integration ist eine Gemeinschaftsaufgabe. Gleichzeitig haben die sozialen Auswirkungen der IT bei 250 Millionen Internetnutzern und über 500 Millionen Smartphone-Nutzern in der EU erheblich zugenommen: Die Stärkung der Sicherheit in der digitalen Gesellschaft liegt damit in der gemeinsamen Verantwortung sowohl des Einzelnen als auch privater und öffentlicher Körperschaften im In- und Ausland. Die Debatte um die zukünftige (digitale) Identitäts-Architektur gehört somit in die breitere Öffentlichkeit und darf nicht mehr nur in Expertenzirkeln geführt werden. Bei Digitalisierung geht es schon lange nicht mehr um den IT-Sektor, sondern vor allem um die Veränderung der Geschäftsabläufe anderer Sektoren.[8]

Aktuell gibt es verschiedene Entwicklungen, die in der Praxis dazu führen, das eine Vielzahl global tätiger Akteure sich damit befasst, die für sie passenden (Geschäfts-) Modelle und die hiermit verbundene Rolle zu finden. Die Diskussion um die Digitalwährung[9] Libra von Facebook

[7] Vgl. https://www.piper.de/buecher/digitaler-humanismus-isbn-978-3-492-05837-7
[8] Quelle: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R(01) p.6ff.
[9] Zu Libra sowie der dahinterstehenden Libra Foundation vgl. bspw. https://www.usnews.com/news/technology/articles/2019-10-23/factbox-facebooks-cryptocurrency-libra-and-digital-wallet-calibra sowie https://libra.org/de-DE/association/ und zur aktuellen Anhörung von Mark Zuckerberg vor dem US-Kongress vom 23. Oktober 2019

zeigt, das es erhebliche Vorbehalte gegenüber Angeboten gibt, die den Staat geradezu herauszufordern scheinen. Gleichzeitig hat der Staat zumindest in den westlich geprägten demokratischen Volkswirtschaften nicht die Befugnis, Dienstleistungen im unmittelbaren Privatbereich seiner Bürger anzubieten. Doch in genau diese Lücke stießen in der Vergangenheit Angebote für proprietäre “Identity Ecosystems” (die Bandbreite reicht hier von Facebook bis hin zu Blockchain Startups), die den tagtäglichen Umgang mit wechselnden Online-Identitäten erleichtern sollten.

Digitale Identitäten sind unabänderlich an Adressen, unter denen sie wiederzufinden sind, gekoppelt, und die Vergabe dieser Adressen und deren Zuordnung zu digitalen Handlungen erfolgt durch den jeweiligen Anbieter. Mit der vollständigen Ausbreitung digitaler, pseudonymer Kommunikationsformen ergeben sich so völlig neue Herausforderungen - und neue Lücken für den mit dem Gesetzgeber immer wieder neu definierten Handlungsraum seiner Bürger.

Aus diesen Erkenntnissen legen wir unseren Vorschlag wie folgt vor: Konkret soll zunächst jedem Bürger die Möglichkeit eingeräumt werden, überhaupt eine digitale Identität (wie etwa im Rahmen der in Estland für jeden EU-Bürger verfügbaren eID) zu beantragen.[10] Hier sollen sowohl (1) Informationen über einen selbst einsehbar (was weiß der Staat in Form der Behörden, was wissen andere über mich?) als auch (2) Informationen für Dritte abrufbar gemacht werden können. Dies soll in einem nächsten Schritt auch für Unternehmen, Vereine und vergleichbare Körperschaften gelten können, die auf diese Art bislang nur mit den Finanzbehörden interagieren. Die erste institutionelle “ID” die einem nach Geburt von den Behörden zugeteilt wird, ist bekanntermaßen die Steuernummer. Es ist aus unserer Sicht dringend erforderlich, das hier nicht nur erweiterte Möglichkeiten, sondern eine grundweg an Fähigkeiten positiv orientierte Nutzerbeziehung realisiert wird, die sich nicht in finanziellen oder rein behördlichen Interaktionsmustern erschöpft.

Denn tatsächlich gibt es ja in Deutschland bereits umfangreichste Datenpools. Da die meisten Daten im urbanen Umfeld sowie bei den neuen Mobilitätslösungen anfallen, bilden die kommunalen Rechenzentren einen der wichtigsten Knotenpunkte. Ein aktuelles Mapping der wichtigsten Datenkooperationen hat aktuell die *stiftung neue verantwortung* erstellt.

Für den regulären Alltags-Nutzer wie mich zählt an erster Stelle der einfache, sichere Umgang mit seiner digitalen Identität dort, wo es notwendig ist (und nirgends sonst). Sprich, ich kann meiner Bank, meinem Vermieter und anderen mein "Führungszeugnis" in Form einer Teil-Sicht auf meinen “Datenschatten” zugänglich machen und habe dabei jederzeit die volle Kontrolle darüber, welche Informationen ich in welcher Form weitergebe, wer sie einsieht und was mit ihnen geschieht, d.h. wie sie beispielsweise weiterverarbeitet werden. Potentiell wäre es interessant, diese "staatlich anerkannte digitale ID" als Anker-ID zu nutzen, um Identitäten bei Diensteanbietern für VideoStreaming, Mobilität etc. bzgl. der Legitimität (Altersnachweis, hat

https://www.washingtonpost.com/technology/2019/10/23/facebook-mark-zuckerberg-testifies-congress-election-libra/

[10] Vgl. bspw. https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/ sowie https://en.wikipedia.org/wiki/Estonian_identity_card für eID

Führerschein, etc.) zu verifizieren (ohne im Sinne der Datensparsamkeit eine konstante Verbindung zu etablieren).

Ein Blick auf ausgewählte Akteure

Selbstverständlich muss eine DIA in der Praxis getestet werden und so designed sein, dass sie sich konsensfähig über die Zeit weiterentwickeln und reifen kann. Ausdruck der aktuell dynamischen Entwicklungsphase ist etwa, dass im Moment noch unbestimmt ist, ob Identifikationsdienste oder Identitätsmanagement relevanter werden: Apple erbringt beispielsweise bei seiner neuen Kreditkarte als wesentliche Mehrwertleistung eine Identifizierungs-Leistung für den Kreditkartenanbieter („card present transaction“). Alle anderen Leistungen sind an den Erwerb und Besitz von Apple Hardware gebunden. Identitätsmanagement würde Apple (und andere, vergleichbare Anbieter) in eine Provider-Rolle und damit Haftung für ggfs. gesetzeswidrige Endnutzerhandlungen bringen. Aktuell reichen die Ambitionen von Apple sogar bis zur Einführung eine eigenen “ePassport”.[11]

Die Unterscheidung zwischen Provider-Rolle und Dienstleistung ist hochrelevant, da sie in der Praxis das auf Daten beruhende Geschäftsmodell[12] so verändert, das der Provider (ohnehin bereits durch eine hohe Regulierungsdichte in Haftung genommen) immer höhere Transaktionskosten und Risiken zu tragen hat, während der ID-Dienstleister die höherwertige Leistung erbringt (wie bspw. Apple gegenüber Mastercard) und durch anteilige Gebühren dazuverdient. Es überrascht daher nicht, dass aktuell eine Mehrzahl von Akteuren daran arbeitet, weltweit ein skalierendes Identifizierungs-System aufbauen, ausrollen und monetarisieren zu können. Digitale Identität bildet hier den äußeren Rahmen während im Kern Identifizierung (iSv Dienstleistung, nicht Provider!) die Wertschöpfung erbringt.

Diese Entwicklung ist allerdings auch von einer gewissen Ambivalenz begleitet, da im “Cloud-Zeitalter” die Erhebung, Speicherung und (Vor-) Verarbeitung der Daten zwar (technisch) dezentral, ihre Zusammenführung und Analyse aber größtenteils zentral organisiert ist. Was im staatlichen Bereich durch Behörden oder im Privatsektor durch Unternehmen geleistet wird, oder eben durch Körperschaften im nicht-staatlichen Sektor oder dgl. hat nunmal immer eine einzige “legal entity”. Auch tendieren sowohl Behörden als auch nicht-staatliche Akteure organisationssoziologisch begründet zu Kompetenzanhäufungen, wie nicht zuletzt gut im Feld des öffentlich-rechtlichen Rundfunks zu beobachten ist. Im “magischen Dreieck der Datenbeziehungen” von Privatleuten, Unternehmen und staatlichen Institutionen gewinnt die Balance zwischen Datenerhebung und Nutzbarmachung der Bürgerdaten an Wichtigkeit. Wir denken, das diejenigen Anbieter erfolgreich sein werden, die kluge Selbstkontrolle und Auskunftspflicht statt Features in den Vordergrund stellen.

---

[11] Vgl. https://www.patentlyapple.com/patently-apple/2018/08/patent-reveals-plans-for-using-apple-pays-secure-element-in-a-future-e-passport-app.html

[12] Für eine vollständige Übersicht des ursprünglichen, auf Adress- und Datenhandel beruhenden Geschäftsmodells und der wichtigsten Anbieter vgl. https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Berichte/Oekon_Wert_Daten_Adresshaendler.pdf?__blob=publicationFile&v=6

Ausblick in eine mögliche Zukunft

Es sei zum Abschluss dieses Beitrags ein Ausblick auf eine mögliche Zukunft mit einer souveränen digitalen Identität gestattet. Während das Zusammenwirken von Selbst- und Fremdbild umfassend beschrieben hat, tritt an ihre Stelle ein neues Dreierverhältnis: Selbstbild, Fremdbild, Netzbild. Zu Beginn sollte der Mensch befähigt werden, einen Abgleich von Selbstbild und Netzbild machen zu können: Die gleichen Algorithmen, die bereits heute für eine Bewertung des Nutzers im Netz eingesetzt werden können, lassen sich auch „privat nutzen, um jeder Person sein Netzbild zu spiegeln: „So sieht das Netz Dich“ wäre die Botschaft einer solchen Analyse. Eine solch digitales Spiegelbild ermöglicht jedem die Reflexion des eigenen Handelns im Netz und die anschließende bewusste Steuerung des Netzbildes. Dieses gespiegelte Netzbild kann im Umkehrschluss für eine Entwicklung der eigenen Persönlichkeit genutzt werden, da das Feedback des Netzes ohne Scham angenommen werden kann. Damit ist der erste Teil der zukünftigen Dreierbeziehung skizziert.

Nun trifft das so bewusst gesteuerte Netzbild auf Dritte, hier zunächst Unternehmen und staatliche Institutionen (u.a. auch Algorithmen). Es sollte dann im Sinne des Nutzers als Souverän seiner digitalen Identität möglich sind, bestimmte persönliche Eigenschaften kenntlich oder unkenntlich zu machen. So sind bestimmte Präferenzen für eine Gespräch mit einem Verkäufer von großer Bedeutung für das Beratungsgespräch. In der digitalen Welt wird dies durch die Auswertung des Profils durch Algorithmen unterstützt. Möchte ich diesen auf mich abgestimmten Angeboten entgehen, schalte ich mein Identitätscockpit aus und das Gegenüber erhält zunächst keine zusätzlichen Informationen über mich. Möchte ich diese Vorauswahl bewusst erreichen, schalte ich das Cockpit entsprechend an. Ein ähnliches Prozedere kann man sich in der Kommunikation mit einer Behörde denken, wie es beispielsweise bei der Steuererklärung bereits möglich ist.

Bleibt der mögliche Einfluss eines digitalen Identitätscockpits für die Allgemeinheit. Wie kann mein digitales Ich dazu beitragen, dass die Gesellschaft sich positiv entwickelt? Hier können wir in einem ersten Schritt Influencer als Beispiel nehmen. Sie haben es durch das Schaffen eines Netzbildes geschafft, andere Menschen dazu zu bringen, ihren Handlungen und Meinungen zu folgen. Allerdings muss diese digitale Aufmerksamkeit in einem weiteren Sinne genutzt werden als lediglich für das Anpreisen von Produkten. So haben bestimmte Youtube Formate mit Lerninhalten bereits eine hohe Bedeutung als alternative Bildungskanäle gewonnen. Den Machern geht es hier (vorrangig) um das Vermitteln von Wissen statt um das Verkaufen von Produkten. Auch Podcast-Sendungen bedienen häufig diesen Wunsch des Menschen nach intellektuellem Wachstum. Damit kann das hier skizzierte Netzbild in der Beziehung zur Gesellschaft auch idealistische Ziele verfolgen. Die Bewegung Fridays for Future beweist dies beispielhaft. Das neue, weltweite Bewusstsein über die Konsequenzen der Erderwärmung wäre ohne eine entsprechende digitale Präsenz der Person Greta Thunberg bzw. der Bewegung nicht in dem Maße möglich gewesen. Wenn wir also in der Lage sind, unser Selbstbild und Netzbild in Einklang zu bringen und dieses auf ein entsprechendes Interesse in der Gesellschaft trifft, kann unser Netzbild eine skalierbare positive Veränderung der Gesellschaft bewirken.

Unsere Vorschläge bezüglich einer Digitalen Identitätsarchitektur, die jedem Einzelnen Transparenz und Auswahl von Optionen und dadurch Kontrolle des Netzbildes ermöglicht, scheint den Zeitgeist zu treffen und wir freuen uns darauf, uns an der gesellschaftliche Diskussion zu beteiligen und hoffentlich auch an der Umsetzung mitzuwirken.