Kommentar zum

Vortrag an den Ministerrat

Bundesgesetz über Sorgfalt und Verantwortung im Netz – digitales Vermummungsverbot vom 10. April 2019

Der Vorschlag für ein „Bundesgesetz über Sorgfalt und Verantwortung im Netz“ zeigt nach wie vor weitgehend ungelöste Probleme des Internet auf:

- Das Internet wird nicht nur von manchen zunehmend für das Verbreiten von Falschinformation, Hass und Diffamierungen missbraucht,
- unabhängig davon steht den Nutzern nach wie vor keine weithin akzeptierte Möglichkeit des Identitätsnachweises gegenüber Diensteanbietern im Internet zur Verfügung.
- Zugleich tracken Werbenetzwerke und einige dominante US-Konzerne nahezu jede unserer Handlungen im Internet
- und bedrohen nicht zuletzt massgebliche Wirtschaftssektoren

„ Ansätze, diese Situation zu verbessern, gibt es.
Es ist höchst an der Zeit, diese umzusetzen “

„Weg von einem Ausweiszwang im Internet, hin zu einer übergreifenden Dachinfrastruktur für die Authentifizierung.“

Zusammenfassung

In der digitalen Welt müssen dieselben Grundprinzipien, Regeln und Gesetze gelten wie in der analogen Welt... (S. Kurz, G. Blümel, et. alt)

Das Funktionieren der Grundprinzipien, Regeln und Gesetze der analogen Welt basiert auf dem über Jahrhunderte gewachsenen **Identitätssystem** unserer Gesellschaft und ist zugleich die Grundlage für den kulturellen, gesellschaftlichen wie volkswirtschaftlichen Fortschritt des Landes. Eingebettet in einem rechtlichen und soziokulturellen Regelwerk, garantiert unser Identitätssystem die Privatsphäre des Einzelnen.

Solange in der digitalen Welt das analoge Identitätssystem **nicht gespiegelt nutzbar ist**, werden Grundprinzipien und Regeln der analogen Welt nur schwer für Diensteanbieter und deren Nutzer vollziehbar sein.

Die Internetnutzung ist heute in der Praxis geprägt von einem „Identifikationsparadoxon“: Einerseits erfolgt schon jetzt kaum einer unserer Schritte im Internet anonym, denn große Werbenetzwerke und die GAFAs verfolgen nahezu alle unsere Aktivitäten, und andererseits steht uns keine weit verbreitete, praktikable und datenschutzfreundliche Möglichkeit zur Verfügung, unsere Identität oder einzelne Attribute daraus glaubwürdig nachzuweisen, wenn wir dies möchten.[1]

Der Gesetzesentwurf, seine zugrundeliegende Problemanalyse, Folgenabschätzung sowie beigefügte Erläuterungen, **fokussieren** sich ausschließlich auf sich häufende strafrechtlich relevante Diskussionsbeiträge in bestimmten Onlineforen[2], deren Ahndung und Verhinderung. Als „Mittel zum Zweck" wird diesen Forenbetreibern eine verpflichtende Identitätsfeststellung des Nutzers beim Registrierungsprozess und damit verbundene **"starke Authentifizierung"** mit Konsequenzen bei Nichterfüllung verordnet (Auslagerung der Authentifizierung an Dritte).

Um gleichermaßen in- und ausländische Diensteanbieter durch das Gesetz erfassen zu können, beruft und stützt sich der Gesetzgeber auf einen Kernbereich des Unionsrechts, genauer gesagt auf die e-Commerce Richtlinie (2015/1535) resp. das österreichische e-Commerce Gesetz (ECG, § 3, Dienst der Informationsgesellschaft)[3], sowie Bundesgesetze des Presse-, Post- und Fernmeldewesen, wodurch sich wiederum Rückschlüsse auf die "gewünschte" - im Gesetzentwurf nicht namentlich bezeichnete - technische Lösung (MobileConnect) und deren **einzubindende Umsetzungspartner** für die geforderte "starke Authentifizierung" und Datenverifizierung ziehen lassen[4]. Nicht zuletzt wird dies durch Nennung der KommAustria/RTR als Aufsichtsbehörde unterlegt.

Der vorliegende Gesetzesentwurf möchte zwar aus Staatsräson positiv dazu beitragen ein von niemanden angezweifeltes negatives Phänomen der heutigen digitalen Welt zu reduzieren, ohne jedoch die wesentlich weiter reichenden ursächlichen Probleme, die der **Ermangelung der Spiegelung des gesamten analogen Identitätssystems** für die digitale Welt geschuldet sind, zu berücksichtigen.

Aus Sicht zahlreicher Experten der Fachbereiche Internetrecht, Datenschutz und IT-Security ist der vorliegende Gesetzesentwurf **nicht geeignet** seiner Intention nachzukommen, da die Basis dazu, nämlich eine strukturierte und umfassende Nutzungs- und Verwaltungsmöglichkeit des digitalen Identitätssystems für den Bürger nach wie vor fehlt.

Im Lichte dessen wäre der vorliegende Gesetzesentwurf ein nicht zu Ende gedachter (fahrlässiger) Schnellschuss, der mehr Schaden als Nutzen für die Demokratie, den Datenschutz, den Umgang mit dem Internet, die Sicherheit

---

[1] Vgl. *Hötzendorfer,* Datenschutz und Privacy by Design im Identitätsmanagement, Österreichische Computer Gesellschaft (OCG), Wien, 2016, S. sowie *Hötzendorfer/Schweighofer*, Die „Identitätskrise“ des Internet, in *Schweighofer/Kummer/Hötzendorfer* (Hrsg.), Transformation juristischer Sprachen. Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012, 2012, S. 429–437.

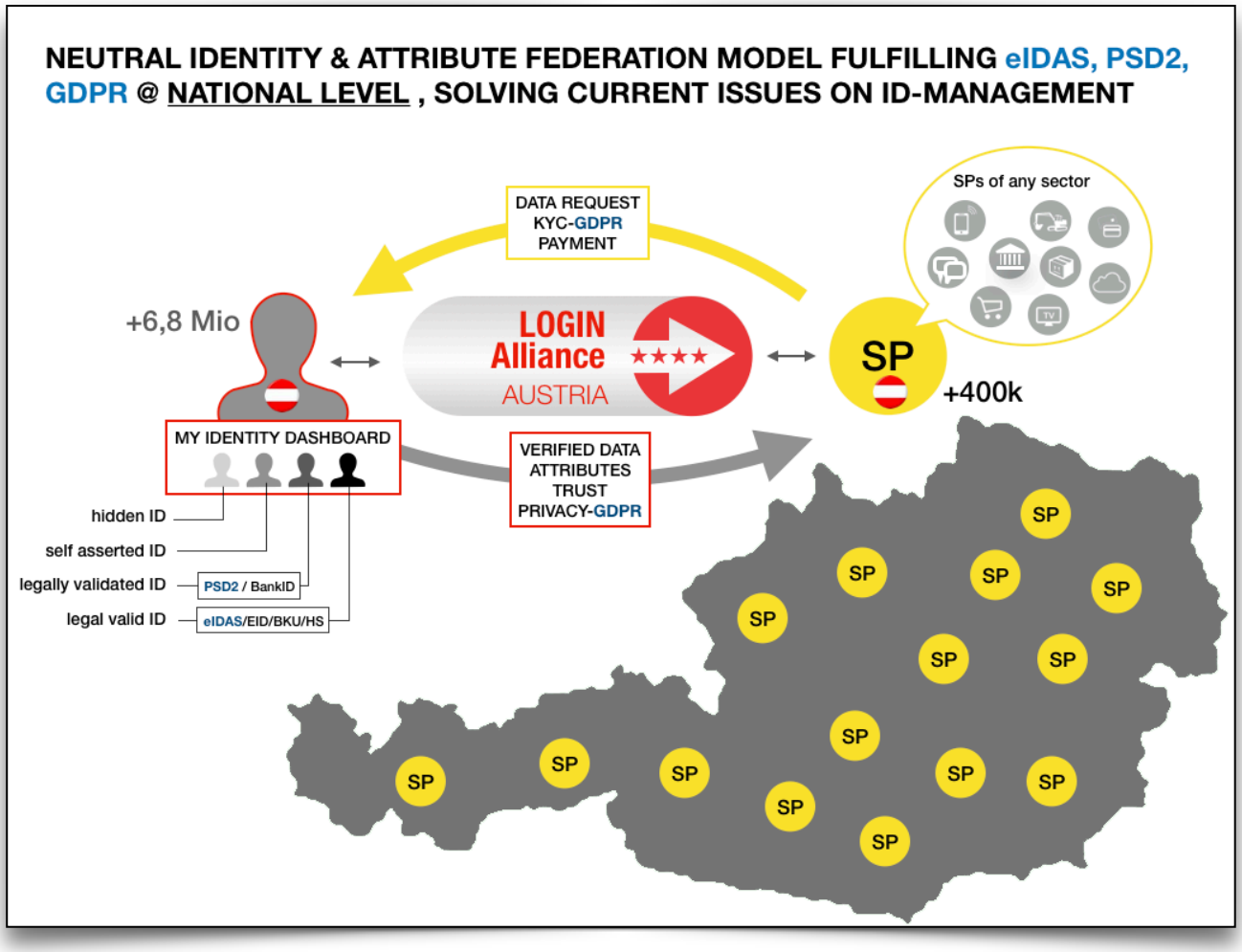
[2] **Eingrenzung des Anwendungsbereichs** auf bestimmte Diensteanbieter mit mehr als 100.000 registrierten Nutzern oder einem jährlichen Umsatz von über 500.000 Euro.

[3] Die **E-Commerce Richtlinie** lässt unter bestimmten Voraussetzungen den Mitgliedstaaten die Möglichkeit, Maßnahmen auch gegenüber ausländischen Anbietern zu ergreifen, wenn dies zum Schutz der öffentlichen Ordnung, insbesondere Verhütung, Ermittlung, Aufklärung und Verfolgung von Straftaten, einschließlich des Jugendschutzes und der Bekämpfung der Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität, sowie von Verletzungen der Menschenwürde einzelner Personen notwendig ist und die Maßnahmen in einem angemessenen Verhältnis zu diesen Schutzzielen stehen.

[4] **MobileConnect** ist ein von der Global System for Mobile Communication - GSMA entwickelter Standard für die Zweifaktor-Authentifizierung mittels SIM oder eSIM des Smartphonesnutzers. Die Authentifizierung läuft über das Netz des Telekombetreibers, die (e)SIM ist ab Vertragsabschluss mit der rechtsgültig geprüften Identität des Endnutzers verbunden. MobileConnect wird in der D-A-CH Region in einigen Federationskonzepten und Single SignOn-Lösungen evaluiert bzw. bereits eingesetzt (Verimi, Log-In-Allianz, et alt.).

anrichtet. Das Thema "Identität im Internet" betrifft JEDE(N) BürgerInn und daher die gesamte Volkswirtschaft des Landes. Es müsste deshalb nur allzu verständlich sein, dass dieses Thema ohne vorangehender vertiefter Diskussion aller Parlamentsparteien und ohne gemeinsamen Schulterschluß nicht "verordnet" werden sollte/darf.

Vielmehr sollte dieser Entwurf nicht nur überdacht, sondern auch den tatsächlich relevanten Problemen des Internet für Bürger und Wirtschaft gegenübergestellt werden. In den weiteren Erläuterungen werden Ansätze aufgezeigt, die bei entsprechender Evaluierung wesentlich effektivere Lösungen anbieten.



Durch Realisierung von bereits vielfach diskutierten Federationsmodellen ließe sich die „Digitalisierung Offensive" des Bundes bis in alle Wirtschaftssektoren erheblich leichter umsetzen, sowie gleichzeitig dazu beitragen datenschutz-relevante Problemstellungen der digitalen Welt zu lösen.

* * * *

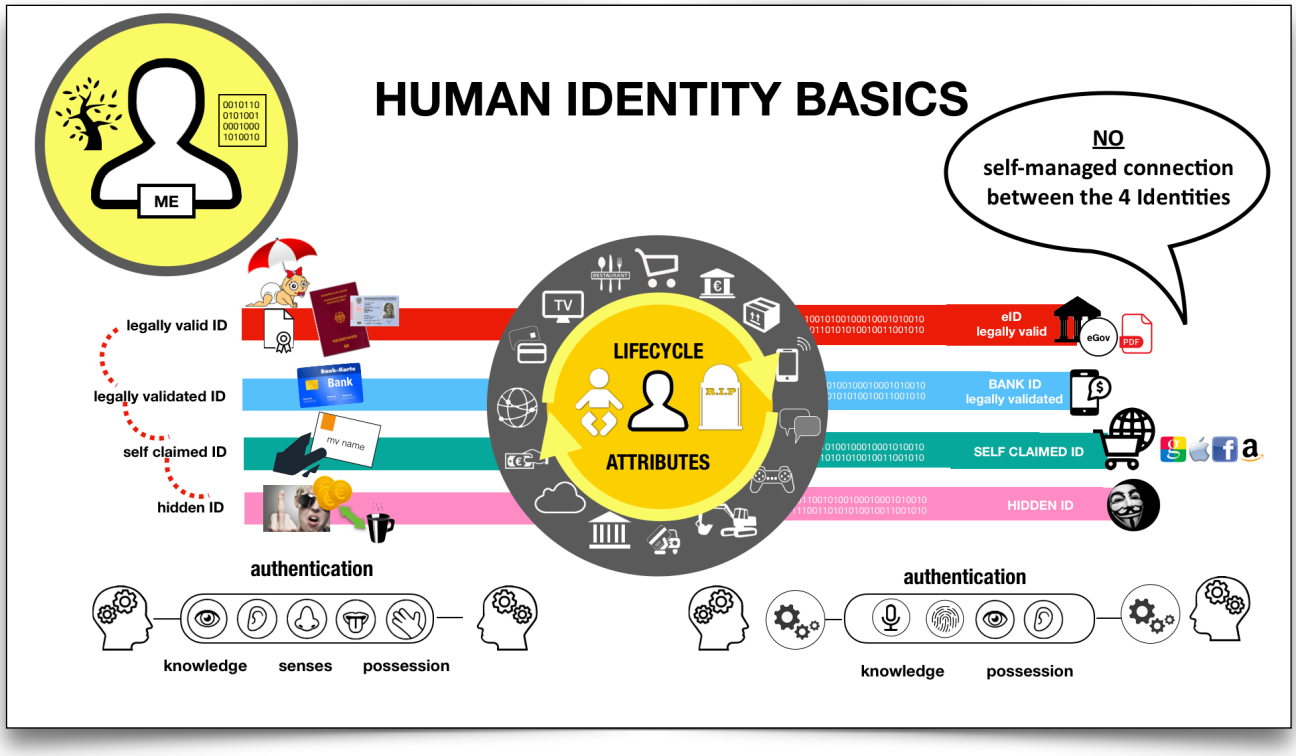
Mag. Heinrich Mautner M.[5]
April 2017

[5] neutraler Querdenker, Unternehmensberater, langjähriger Experte und Initiator für digitale Identitätsmanagement Konzepte und IT-Architekturen, die die EU-weiten Regelungen (eIDAS, PSD2, DSGVO) mit nationalen Gesetzen (eGOV, VertrauendiensteG, TelkG, etc) sowie internationalen Bestrebungen zur Schaffung globaler Authentifizierungsstandards (FIDO-Alliance, MobileConnect-GSMA, W3C) und Federierungsframeworks wie OpenID, SAML, oAuth und Technologien wie Ledger Technology, Blockchain in sich vereinen. HMM ist Mitinitiator des Arbeitsprojektes "StarTrust Alliance-Austria/EU" (zuvor TelcoFed-Austria - A1, T-Mobile, Hutchison Drei), eines umfassenden Konzeptes/Modells einer national strukturierten Identitäts- & Attribute Federation, Mitgründer und Präsident des Institute for Digital Privacy (IDP), sowie Mitglied des Arbeitskreises "Wirtschaftsportalverbund" Austriapro/WKO.

Weitere Erläuterungen

Das analoge Identitätssystem besteht aus 4 (vier) Identitätsformen die es dem BürgerIn ermöglichen die Privatsphäre zu leben, abzugrenzen und zu schützen. Es gilt zu unterscheiden:

1. die **rechtsgültige Identität**, die vom Staat erhoben und verwaltet wird (Geburt, Reisepass, Personalausweis,..),
2. die **rechtsgültig geprüfte Identität**, die von bestimmten Wirtschaftsunternehmen per Gesetz/EU-Regulierung durchzuführen ist, auf der Authentifizierung der rechtsgültigen Identität beruht und deren Daten zwecks Aufrechterhaltung oder Errichtung einer Kundenbeziehung gespeichert werden (Bankkonto, Telko-Vertrag),
3. die **selbstbehauptete** (*zB. Grüß Sie, Ich bin der XY...*) und
4. die **verdeckte Identität** (*zB. Ware gegen Geld*), die beide jedem BürgerIn ganz wesentlich den Schutz der eigenen Privatspäre ermöglichen und ungeteilt von diesem(r) "verwaltet" und im Alltag am öftesten genutzt werden.



Die Rahmenbedingungen, welche Identität "genutzt" wird, geben Gesetze, die Marktwirtschaft und die Gesellschaft selbst vor (Identitätsfeststellung, Ausweispflicht, gesellschaftlicher Umgang). Jede dieser Identitätsformen wird von Geburt an bis zum Tod durch Attribute "angereichert" bzw. diese von Dritten "zugeordnet". Identitätsattribute entstehen, ändern sich, verschwinden oder werden gelöscht (Lifecycle Attributes). Als **Authentifizierungmittel** stehen uns im analogen Alltag unsere Sinne, unterstützt vom Verstand/Gedächtnis zu Verfügung im Internet werden Computer dazu herangezogen. Alle 4 Identitätsformen sind im analogen Leben miteinander vernetzt. (Bsp.: Verübt jemand (anonym) einen Raub und wird dabei beobachtet (Sinne), so kann der Täter vom Beobachter der Exekutive "beschrieben" und von dieser festgenommen und identifiziert werden...) Die Verknüpfung ist daher zwischen den Identitätsformen **verdeckt** - **selbstbehauptet** - **rechtsgültig geprüft** - bis zur **rechtsgültigen Identität** gegeben.

Im digitalen Raum ist eine Vernetzung bis heute nicht gegeben. Dies führt zu[6]:

- ➡ **Mangelnder Transparenz und Kontrolle**
- ➡ **Mangelnder Datenschutz**
- ➡ **Mangelnder Komfort**
- ➡ **Mangelnde Sicherheit**
- ➡ **Mangelnde Nachweismöglichkeit**

[6] Vgl. *Hötzendorfer,* Datenschutz und Privacy by Design im Identitätsmanagement, Österreichische Computer Gesellschaft (OCG), Wien, 2016 - Identität im Internet S 21-27

Die Auslagerung von "Authentifizierungsprozessen" und/oder der "Datenverifizierung" aus dem alleinigen Verantwortungsbereich des Diensteanbieters an Dritte (Identitätsservice Provider) ist in einigen nationalen wie internationalen Konzepten und Modellen geforderte Maßnahme eines zukunftsorientierten und alle Identitätsformen umfassenden digitalen Identitätsmanagements, sofern dadurch die Interessen und Privatsphäre des Bürgers sowie der Datenschutz insgesamt gesichert sind (Stichwort: Identitäts & Attribute Föderationsmodell).

- *Verpflichtung für Diensteanbieter, die Foren betreiben bzw. die Einrichtung eines Forums ermöglichen, dafür Sorge zu tragen, dass die Identität des Posters festgestellt und überprüft wird. Erst nach erfolgreichem Abschluss des Registrierungsprofils können Postings in diesem Forum veröffentlicht werden.*

- *Nutzer haben ein Registrierungsprofil zu erstellen und ihren Vornamen, Nachnamen sowie Adresse anzugeben, sowie einen öffentlich sichtbaren Nutzernamen.*

Im gegenständlichem Fall wird in den privatwirtschaftlichen Bereich (Mediensektor) und die Privatsphäre des Bürgers eingegriffen und eine Verifizierung der Identität bei der Authentifizierung verlangt, die von der bisher ausreichend erachteten "selbstbehaupteten Identität" abweicht.

Zu meinen, an einer einzigen Schraube drehen zu müssen, um ein Problem losgelöst von den übrigen Problemen lösen zu können, ist nicht nur kurzsichtig, sondern schafft wiederum neue Probleme an anderen Stellen und vermag bestehende schwerwiegendere Probleme in anderen Onlinebereichen nicht (mit)zu lösen.

Die geforderte stärkere Authentisierung und Authentifizierung, verknüpft mit verifizierten Identitätsdaten die von u.A. dritten Dienstleistern zu erheben und zu speichern sind, schafft keine Vorteile zur gegenwärtigen Situation in zB. Foren, solange keine dem analogen Identitätssystem angepasste digitale Identitätsmanagementstruktur auf breiter Basis für ALLE Internetteilnehmer sichergestellt wird. Im Gegenteil, eine derartige Verpflichtung schafft wiederum neue unnötige Datensilos bei Betreibern verbunden mit hohen betrieblichen Aufwendungen.

Es ist höchste Zeit die vielfach vorliegenden und bereits mit direkt und indirekt involvierten Stakeholdern[7] intensiv diskutierten Lösungsvorschläge heranzuziehen, um gesetzliche "Schnellschüsse" auf politischer Ebene zu überdenken. Die geltenden EU-Regulierungen, Gesetze und Verordnungen[8], sowie internationale Bestrebungen, nämlich einen Authentisierungs- und Authentifizierungsstandard (W3C, FIDO-Alliance, GSMA) global zu etablieren, sind in einigen der vorliegenden Konzepte zur Schaffung geeigneter national (und EU-28) ausgerichteter Strukturen für ein durchgreifendes und zukunftsorientiertes digitales Identitätsmanagement bereits berücksichtigt und bedürfen nun einer breiteren politischen Diskussion für die weitere Entscheidungsfindung. Nationale Alleingänge ohne Berücksichtigung und Einbindung internationaler Standards sind zum Scheitern verurteilt, vor allem dann, wenn das digitale Identitätssystem nicht ebenso national strukturiert ermöglicht wird und den/die BürgerIn und seine/ihre Privatsphäre in den Mittelpunkt stellt wie es im analogen Identitätssystem der Fall ist.

Vielmehr sollte es so sein, dass der wesentlichste Teil der Identitäts-Management-Prozesse wie die Authentifizierung den Diensteanbietern (International/national) **ENTZOGEN** und jeweils auf nationaler Ebene von einem **neutralen Identitäts- & Attribute Federationsmodell** (siehe Darstellungen) durchgeführt wird. Eine auf die nationale ID-Datensammlerstruktur (Staat, Banken, Telkos, BürgerIn) aufgesetzte IT-Architektur mit ineinandergreifendem neutral organisierten Authentifizierungsdiensten und einer Aufsichtsbehörde macht das sich wiederholende Datensammeln bei Diensteanbietern obsolet (Privacy by Design), stärkt die heimische Wirtschaft, bewahrt die Privatsphäre des Nutzers und kann als Show Case für einen EU-weiten RollOut dienen. Im vorliegenden Gesetzesentwurf wird die KommAustria /RTR als Aufsichtsbehörde offensichtlich deshalb definiert, weil für die Authentifizierung das mobileConnect-Verfahren[9] (zweiter Faktor SIM-Karte und/oder eSIM) herangezogen werden soll, also eine bestimmte

[7] BKA, BR, eGov, Ministerien BMI, BMDW, BMF, BMBWF, AK, WKO, IV, Bundesrechenzentrum, Post AG, Kontrollbank, STUZZA, Nationalbank, ISPA, Bankenverband, Handelsverband, RTR, Telkos, Hauptverband, Versicherungen, Datenschutzorganisationen, et alt.

[8] DSGVO, PSD2, eIDAS, Urheberrecht, eGov, VertrauensdiensteVO, TelKG, Passwesengesetz, SignaturG, etc

[9] MobileConnect ist ein von der Global System for Mobile Communication - GSMA entwickelter Standard für die Zweifaktor-Authentifizierung mittels SIM oder eSIM des Smartphonesnutzers. Die Authentifizierung läuft über das Netz des Telekombetreibers, die SIM ist ab Vertragsabschluss mit der rechtsgültig geprüften Identität des Endnutzers verbunden. MobileConnect wird in der D-A-CH Region in einigen Federationskonzepten und Single SignOn-Lösungen evaluiert bzw. bereits eingesetzt (Verimi, Log-In-Allianz).

Technologie bevorzugt wird. Telekommunikationsbetreiber gelten wie Banken auch als Identitätsservice Provider für die "rechtsgültig geprüfte" Identität ihrer Kunden und könnten diese Daten während eines Registrierungsprozesses des Nutzers mit dessen Zustimmung an Diensteanbieter weitergeben (= Federieren).

Im Wirkungsbereich des Staates (eGovernment, eIDAS, E-ID) findet eine solche Auslagerung (eigentlich Aufteilung)[10] von hoheitlich geführten Prozessen zur sicheren Abwicklung der digitalen Kommunikation zwischen Staat und Bürger bereits statt (oesterreich.gv.at), die Authentifizierung betrifft jedoch nur jene vom Staat verwaltete "rechtsgültige Identität" des Bürgers. In weiteren Ausbaustufen (E-ID) ist die Erweiterung von bisher staatlich erhobenen bereichsspezifischen Personenkennzeichen (bPK) aus Registern vorgesehen und deren Nutzung für den privatwirtschaftlichen Sektor vorbereitet. Ebenso werden Möglichkeiten ausgelotet[11], die es dem Bürger(in) ermöglichen neben staatlich verwalteten Attributen (Führerschein, Personalausweis, etc), weitere - auch selbstbehauptete - Attribute mit der eigenen E-ID zu verbinden und in Folge an eine Nachfrageseite weiterzuleiten.

Dies ist fast im Sinne eines strukturierten ID-Federationsmodells, jedoch muss ZUERST

ein übergeordnetes Trust Framework mit entsprechender Rollenverteilung und Schnittstellen-Architektur für alle Federationsteilnehmer (Identitätsservice Provider, Attributeservice Provider, neutraler Authentifizierungsdienst, Datennachfrageseite/Onlinediensteanbieter, Dateninhaber/Endnutzer und Aufsichtsbehörde) geschaffen werden, um die Spiegelung des analogen Identitätssystems in die digitale Welt sicher, vertrauensvoll und neutral ausgerichtet zu gewährleisten. Die in diesem Gesetzesentwurf festgelegte Lösung - auch wenn mobileConnect nicht ausgesprochen wird - ahmt nichts anderes als die vielfach bekannte "Facebook-Connect" Lösung nach, die sich aus heutiger Sicht als entbehrlich - ja nahezu die Demokratie gefährdend - darstellt.

Die Meinung, dass der Staat die Allmacht über das gesamte analoge wie digitale Identitätssystem innehat, ist ebenso naiv und zum Scheitern verurteilt[12] wie die Annahme, dass durch dieses Gesetz den BürgerInnen und der heimischen Wirtschaft Gutes getan wird. Vielmehr ist es notwendig **transparente Strukturen** zu schaffen die den Schulterschluss zwischen den Stakeholdern, sowie eine vertrauensvolle, sichere und einfache Nutzung des digitalen Identitätssystems ermöglichen. Erst ab Realisierung derartiger Strukturen werden sich mit Identitäten & Attribute verbundene rechtliche, gemeinschaftliche, wirtschaftliche wie auch gesellschaftliche Notwendigkeiten und Probleme für die digitale Welt lösen lassen.

In der digitalen Welt müssen dieselben Grundprinzipien, Regeln und Gesetze gelten wie in der analogen Welt... (S. Kurz, G. Blümel, et. alt)

Nach nunmehr ±30 Jahren hat sich das kommerzialisierte Internet als DER digitale Kommunikationskanal global etabliert, dies jedoch ohne Übertragung des analogen Identitätssystems in diese rasant wachsende digitale Welt. Dieses Versäumnis stellt uns heute vor nahezu "vorprogrammierte" Probleme, die allzuoft das Internet als "rechtsfreien Raum" darstellen wollen, was es jedoch nicht ist. Einige wenige global agierende "Internet-giganten" (GAFAs) konnten entstehen und jene von Nutzern zu Verfügung gestellten, vorwiegend "selbstbehaupteten und verdeckten" Identitäts- & Attributdaten mit den digitalen Footprints vernetzen, analysieren und teilanonymisiert vermarkten. Die Fülle der den GAFAs dazu bereitstehenden Datenquellen sind zu ID-Ecosystemen herangewachsen und erschweren Marktteilnehmern außerhalb dieser ID-Ecosysteme zu reüssieren.

Die, heute eklatant gewordenen Probleme wie Identitätsdiebstahl, Verstöße gegen die Privatsphäre, online Demütigungen, Steuerflucht/-Ungerechtigkeiten, die (Markt-)Macht der GAFAs über die gedeihliche Entwicklung des eCommerce innerhalb des Binnenmarktes und innerhalb seiner Volkswirtschaften, bis hin zur Bedrohung einzelner Wirtschaftssektoren sind der Ermangelung von national strukturierten und für jede(n) BürgerIn zugänglichen digitalen Identitätsmanagement geschuldet.

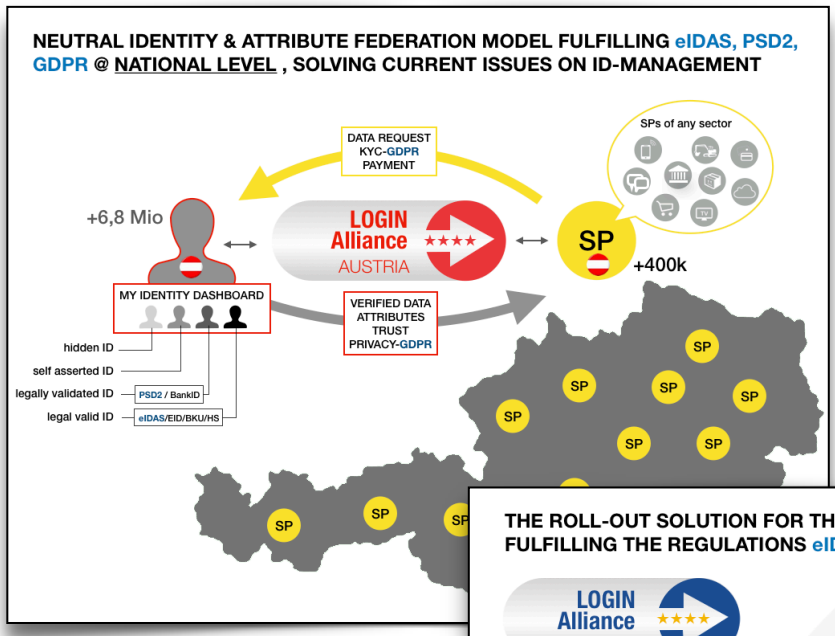
---

[10] hier ist die Anmeldung des Bürger mittels Handy-Signatur (Bürger - ATrust - Register) bzw. die Datenfederierung zwischen Registern, Behörden, etc und Applikationen innerhalb der eGovernement Prozesse gemeint. Die im Aufbau befindliche E-ID (Elektronischer Identitätsnachweis) wird in das derzeitige System integriert.

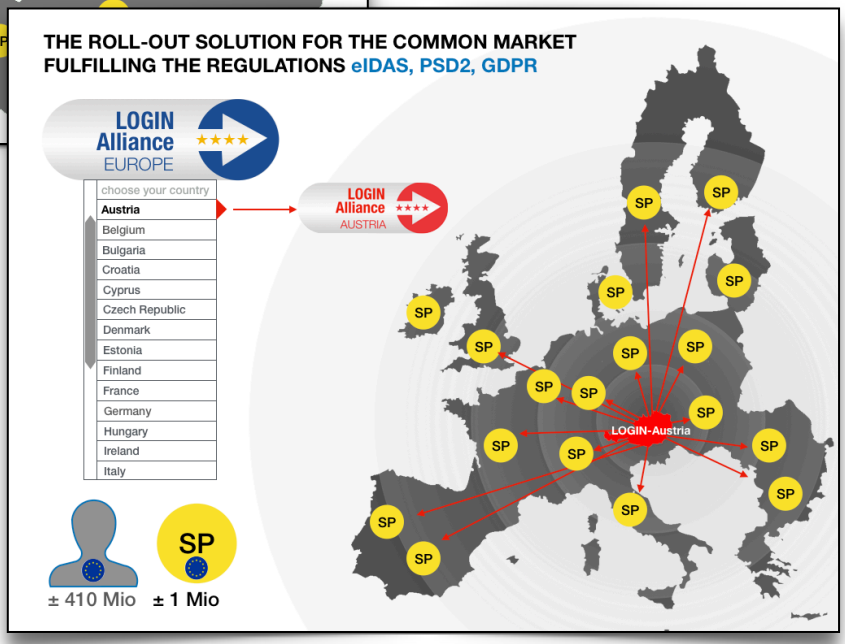
[11] 29.04.2019 Referat R.Ledinger, Geschäftsführer der Plattform und Bereichsstellvertreter und interimistischer Leiter der Gruppe B (Abteilungen I/B/4 bis I/B/7) im Bundesministerium für Digitalisierung und Wirtschaftsstandort, anlässlich Veranstaltung "Agenda Austria 2035"

[12] Anzahl der Authentifizierungen mittels Handysignatur pro Jahr ± 10 Mio (rd. 30.000 tägl.Nutzungen). Anzahl der Authentifizierungen österreichischer Internetnutzer (6,8 Mio) gegenüber Service Providern (national & international) pro Jahr ± 15 Milliarden. Davon stehen ± 70% Authentifizierungen zu internationalen Diensten lediglich 30% heimischen Diensten (Foren, eCommerce) gegenüber.

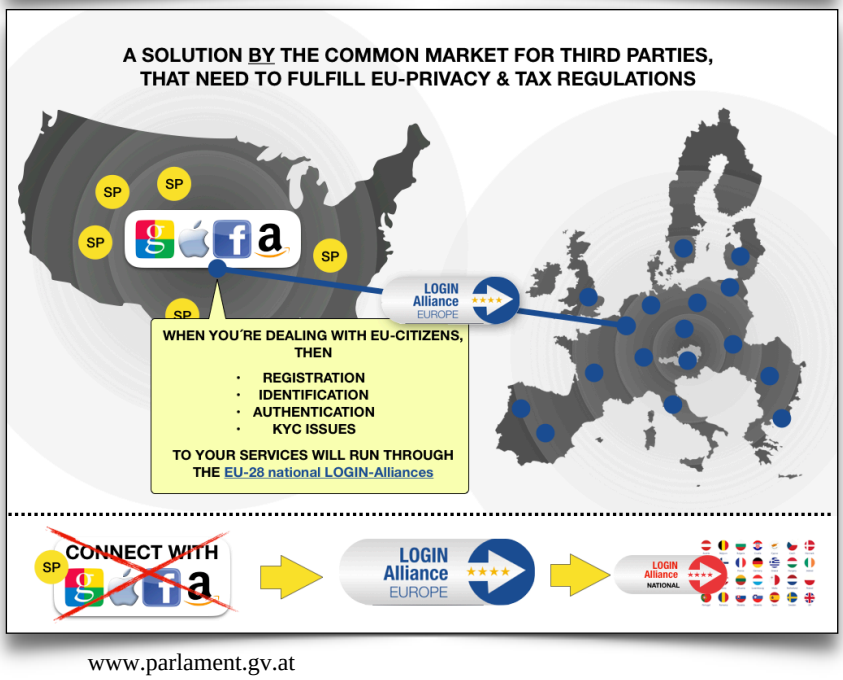
Ohne breit ausgerollter nationaler Identitätsmanagementstruktur wären heimische Diensteanbieter nicht nur technisch wie finanziell überfordert, sondern diesem Gesetz nicht unterliegende übrige Diensteanbieter benachteiligt, gleichzeitig die Großen (GAFAs) bevorzugtn. Der vorliegende Gesetzesentwurf würde dazu führen, dass die GAFAs noch mehr personenbezogene Daten erhalten und speichern dürfen, als das bisher der Fall ist. Facebook, das mit der Durchsetzung der selbst festgelegten Klarnamenpflicht teilweise gescheitert ist, kann sich eine staatliche Klarnamenpflicht nur wünschen. Der Staat sollte aber keinesfalls dazu beitragen, dass diese US-Unternehmen noch mächtiger werden.



Das Modell einer "**national strukturierten Identitäts- & Attribut Föderation**" ermöglicht de(r)m Bürger(In) seine (ihre) Identitätsformen zu verwalten, sowie der Wirtschaft geltende Gesetze (DSGVO, eIDAS, PSD2) leichter zu erfüllen, als auch bestehende Schwierigkeiten des eCommerce zu überwinden.



Dasselbe Föderationsmodell wäre in jedem EU-Mitgliedsstaat realisierbar und würde den „digitalen Binnenmarkt" wesentlich erleichtern.



Die an nationale Identitätslösungen „ ausgelagerte Authentifizierung" des Nutzers bewirkt, dass Service Provider aus Drittstaaten ihre ID-Ecosysteme überdenken müssen, um ihre Dienste den EU-Gesetzen konform (DSGVO, eIDAS, PSD2, eCommG, et alt.) anbieten zu können.