Elektronische ID: eine für alle(s)?

Zusammenfassung

Die Einführung einer digitalen europäischen Identität soll eine Vereinheitlichung bringen und den BürgerInnen Europas ermöglichen, sich unproblematisch und sicher im digitalen Raum zu bewegen. Gleichzeitig soll so ein e-Identity-Ökosystem entstehen, das europäische KonsumentInnen und Firmen aus der Abhängigkeit von großen US-amerikanischen Plattformen befreit. Seit Juni 2021 liegt eine Empfehlung der EU-Kommission vor, wonach bis 2030 die e-Identität (eID) allen EuropäerInnen zur Verfügung stehen soll. Abseits der angestrebten Ziele stellen sich allerdings einige offene Fragen bezüglich der grundsätzlichen Wünschbarkeit, mancher Risiken und vor allem der technischen Umsetzung. So ist folgendes nicht abschließend geklärt: Ist *eine* Identität tatsächlich sozial wünschenswert? Wie sollen unterschiedliche Identitäten für unterschiedliche Rollen wie z. B. BürgerIn (staatlich, anonym/nicht-anonym) oder KonsumentIn (privat, anonym/pseudonym/nicht-anonym) realisiert werden? Wie können der Datenschutz und die Grundrechte auf Privatsphäre und freie Meinungsäußerung gewahrt werden? Und wie kann der zu erwartende Digital Divide zwischen NutzerInnen und jenen BürgerInnen, die sich dieser Anwendung verschließen oder aus unterschiedlichen Gründen nicht fähig sind daran teilzunehmen, verhindert werden?

Überblick zum Thema

Aufwändiges Identitätsmanagement im virtuellen Raum

Die Digitalisierung vieler Lebensbereiche hat zur Folge, dass immer mehr BürgerInnen Zugänge zu öffentlichen und privaten e-Services nutzen. In vielen Fällen wird eine Identifizierung verlangt, die unterschiedlich eng an der realen Identität angelehnt sein kann: von einfachen Benutzerkennungen und Pseudonymen mit frei gewählten Passwörtern bis zur quasi staatlich zertifizierten Identifizierung mit der elektronischen (Handy-)Signatur. Diese Vielzahl von Anwendungen hat zur Folge, dass für BürgerInnen aber auch für Institutionen ein aufwändiges Identitätsmanagement notwendig geworden ist. Man/ frau kann sich auf die Sicherheits- und Speichereinstellungen des Browsers oder des Smartphones verlassen oder sich gleich einer bestimmten Identität – oft einer Plattform aus dem Social-Media-Bereich oder eines Marktplatzes einer der Tech-Firmen – bedienen. Dem soll durch eine Initiative der EU-Kommission entgegengewirkt werden.

Vorschlag der EU-Kommission für eine europäische eID

Anfang Juni 2021 hat die EU-Kommission eine Empfehlung (2021/946)[1] für den Weg zu einer europäischen digitalen Identität (eID) herausgegeben. In dieser beschreibt sie die Zielsetzung und den zeitlichen Rahmen zur Entwicklung einer europäischen digitalen Identität. Die Empfehlung zielt darauf ab, einen strukturierten Prozess der Zusammenarbeit zwischen den

[1] eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2021.210.01.0051.01.DEU&toc=OJ%3AL%3A2021%3A210%3ATOC.

Mitgliedstaaten, der Kommission und gegebenenfalls den Akteuren des Privatsektors zu schaffen. Dieser Vorschlag basiert auf der seit 2014 bestehenden eIDAS-Verordnung (910/2014)[2] und führt diese weiter. Herzstück soll eine sogenannte elektronische Geldbörse (eWallet) sein. Mit Hilfe der im eWallet gespeicherten Daten sollen sich die EU-BürgerInnen schnell und sicher ausweisen und Zutritt in der digitalen Welt verschaffen können. Die europäische digitale Identität für Online-Interaktionen und -Präsenz soll den BürgerInnen bis 2030 zur Verfügung stehen.

Die eWallets sollen für unterschiedliche Services genutzt werden können

Die eWallets sollen für Identitätsangaben (v. a. auch grenzüberschreitend) genutzt werden (Adressen, Alter, Geschlecht, Personenstand, Familienzusammensetzung, Staatsangehörigkeit, Ausbildung, Berufsqualifikationen und Titel, Erlaubnisse und Lizenzen, andere Genehmigungen und Zahlungsdaten). Allein der Umfang der in den eWallets möglicherweise gespeicherten Daten lässt KritikerInnen dieses Vorhabens aufhorchen und Datenschutzbedenken äußern (Lutz 2020).

Die eIDAS-Verordnung von 2014 hatte die gegenseitige Anerkennung von digitalen Ausweisen und Zertifikaten innerhalb der EU zum Zweck. Nun soll isolierten nationalen Ambitionen und damit der Fragmentierung derartiger Lösungen entgegnet werden. Bis Ende Oktober 2022 soll das Instrumentarium samt den technischen Anforderungen, Architektur etc. durch die Kommission veröffentlicht werden.

Der Anspruch ist Sicherheit und Vertrauen für Europäische BürgerInnen …

In der State-of-the-Union-Ansprache 2020[3] wies Kommissionspräsidentin van der Leyen darauf hin, dass oft unklar bliebe, was nach einer Anmeldung in verschiedenen Systemen, wie Apps und Webseiten, mit den Daten geschehe. Dem wolle die Kommission mit dem Vorschlag einer sicheren e-Identity entgegentreten und den BürgerInnen mehr Kontrolle über ihre Daten ermöglichen.

… und ein Gegengewicht zur US-amerikanischen Tech-Firmen

Neben Themen wie Vereinheitlichung, besseren Voraussetzungen für den digitalen Binnenmarkt und Bequemlichkeit für die BürgerInnen und KonsumentInnen ist also auch die Frage der Datenverwendung, des Datenschutzes und vor allem die Schaffung eines europäischen digitalen e-Identity-Ökosystems[4], ein Ziel dieses Vorhabens. Damit soll die Unabhängigkeit von großen US-amerikanischen Tech-Firmen wie Google, Amazon, Facebook, Microsoft und Apple etc. für Behörden, Unternehmen und BürgerInnen ermöglicht werden. Auch in anderen Bereichen der Welt wird an Identifikationssystemen gearbeitet. Die Weltbank hat 2014 das Programm „Identification for Development“ ins Leben gerufen, mit dem Ziel, Menschen in Entwicklungsländern besseren Zugang zu öffentlichen Leistungen wie Sozialsystem und Bankwesen zu ermöglichen. Ähnliche Initiativen gibt es auch seitens der Vereinten Nationen (Johnson/Campbell 2020). Eine weitere Initiative ist die u. a. von Microsoft, der Gates-Stiftung und

[2] eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014R0910&qid=1634046882917.

[3] ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655.

[4] Ein e-Identity Ökosystem wird i.d.R. die Gesamtheit von Akteuren, Technologien, Regulierungen und Anwendungsfällen genannt.

Accenture finanzierte „Digital Identity Alliance ID 2020“, ein Public Private Partnership, das durch Schaffung eines Systems für transnationale digitale Identitäten, Reisefreiheit und Rechtsfähigkeit von Personen und damit etwa Zugang zu staatlichen Leistungen und digitalen Diensten stärken will.[5] Die ID-2020-Allianz ist jedoch nicht unumstritten. Kritikpunkte an der Allianz sind die Entwicklung intransparenter proprietärer Technologien und die starke Rolle der involvierten Konzerne und Stiftungen, womit u. a. Risiken einer Kommerzialisierung staatlicher Aufgaben wie jener der Identifizierung von BürgerInnen und der Verwaltung von Identitätsdaten verbunden sind (Wagner 2020). So können gerade in Entwicklungsländern Technologien im größeren Stil getestet werden, ohne an Datenschutz- und Sicherheitsstandards in Europa oder auch den USA gebunden zu sein.

Seit dem Aufkommen der Social Media Plattformen haben sich eine Vielzahl derartiger privater e-Identity-Systeme etabliert, was dazu geführt hat, dass durch Netzwerkeffekte die Großen noch größer werden. NutzerInnen können sich nun bei vielen e-Services mittels einer Identität einer der großen Plattformen anmelden. Wer diese nutzt, setzt sich potenziell breiter Nachverfolgung und Überwachung aus. Wer sie nicht nutzt, hat extra Mühe aufzuwenden, eine Vielzahl von e-Identities aus unterschiedlichsten Services sicher zu verwalten (Engemann 2015). Deshalb klingt der Ansatz der EU-Kommission vielversprechend und soll die Nutzung einfacher und sicherer machen. Einen Verstärkungseffekt hat in diesem Zusammenhang sicher auch der „Digitalisierungsboost“, der durch COVID-19 entstanden ist (u. a. durch die digitalen COVID-Zertifikate). Die Lehren, die europaweit daraus gezogen wurden, sollten in das Design der e-Identity jedenfalls einfließen.

Grundsätzlich stellt sich aber die Frage, wie wünschenswert eine elektronische Identität ist.[6] Im analogen Bereich sind wir es gewohnt, in unterschiedlichen Rollen zu agieren und auch unser Verhalten der konkreten Situation und Rolle anzupassen. Zutritt zu Kulturveranstaltungen erhält man i.d.R. (zumindest in Vor-Pandemie-Zeiten) in anonymer Form allein durch Vorweisen der gültigen Eintrittskarte. Es wird also nicht die Identität, sondern nur die Berechtigung, eine bestimmte Dienstleistung zu nutzen, überprüft. Wird durch ein staatlich verifiziertes bzw. garantiertes Angebot wie die eID der Zutritt zu digitalen Angeboten zunehmend von der eID geprägt sein? Wird es möglich sein, weiterhin ohne eID bestimmte Dienste in Anspruch zu nehmen? Die Verwendung von Pseudonymen, von unterschiedlichen Rollen im Zusammenleben, soll mit der eID möglich sein. Wie aber werden diese unterschiedlichen Rollen in der technischen Umsetzung der eID realisiert werden und wie kann technisch sichergestellt werden, dass von unterschiedlichen Rollen nicht auf die zugrundeliegende Identität bzw. andere Rollen geschlossen werden kann? Insbesondere der gesamte Bereich der Cybersecurity im e-Identitätsmanagement erscheint derzeit noch unklar.

Offenen Fragen:

Braucht es eine e-Identity überhaupt?

[5] id2020.org.

[6] privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id.

Wie Privatsphäre und freie Meinungsäußerung schützen?

Weitere offene Fragen betreffen die mögliche Einschränkung wesentlicher Grundrechte wie jenes auf Privatsphäre und jenes auf freie Meinungsäußerung – deren konkrete Umsetzung zu einem großen Teil auf dem Recht auf Anonymität im öffentlichen Raum fußen.[7] Wird die einfache Anwendung von eID-Prozessen zur Überwachungsmaschine (Kruchem 2020) bzw. befördert sie über den bekannten „function-creep"[8] Begehrlichkeiten bei Institutionen und Unternehmen? Nicht zuletzt die Beantwortung dieser und ähnlicher Fragen wird zur Akzeptanz oder Ablehnung der eID führen. Nach dem derzeitigen Diskussionsstand soll die eID freiwillig sein. Wie wird in Begleitmaßnahmen sichergestellt, dass BürgerInnen, die das nicht wollen oder können, nicht benachteiligt werden und es nicht zu einem Digital Divide kommt (Cater 2021).

Informationsasymmetrie und Machtgefälle der Beteiligten

Die eWallets sollen neben den für die Identitätsfeststellung notwendigen Daten auch um weitere Attribute angereichert werden können. Dabei ist insbesondere darauf Bedacht zu nehmen, dass institutionelle Anbieter und Nutznießer derartiger Verfahren (insbes. Plattformbetreiber, Unternehmen, Behörden) grundsätzlich mehr Kontrolle über die verarbeiteten Daten haben, als die Betroffenen. Biometrische Daten erhöhen diese Form von Informationsasymmetrie, die individuelle Identitäten betrifft, erheblich (Strauß 2019). Insbesondere die Verquickung hoheitlicher Identifikation mit privatrechtlichen Anbietern und Services erscheint problematisch und sollte nur sehr restriktiv gehandhabt werden.

Biometrische Daten sind besonders problematisch

Bezüglich der technischen Gestaltung ergeben sich auch noch eine Reihe offene Fragen (Lomas 2021). Insbesondere der Grad der Zentralisierung von Daten gegenüber einer dezentralen Systemgestaltung muss vor dem Hintergrund möglicher Überwachung diskutiert werden. Aufgrund ihrer engen Bindung an eine bestimmte Person drängt es sich quasi auf, biometrische Daten in eine eID einfließen zu lassen. Aufgrund mancher problematischen Eigenschaften biometrischer Daten (Schaber et al. 2020) – wie etwa die Nicht-Veränderbarkeit, die bei Identitätsdiebstahl die Folgen potenziell vervielfachen – sollte jedoch davon abgesehen werden.

Relevanz des Themas für das Parlament und für Österreich

ID-Austria und europäische eID in Einklang bringen

In Österreich ist mit der Änderung des e-Government-Gesetzes, des Passgesetzes 1992, des Führerscheingesetzes und des Kraftfahrgesetzes 1967[9] bereits Ende 2020 die gesetzliche Grundlage für die Einführung der ID-Austria (IDA)[10] gelegt worden. Die IDA soll in weiterer Folge die bestehende Bürgerkarte ablösen. Für die konkrete Ausgestaltung und Weiterentwicklung wird es notwendig sein, die Prozesse auf europäischer Ebene

[7] Siehe dazu nach wie vor das wegweisende Urteil des BVerfGE (1983).

[8] Darunter wird die schrittweise Ausweitung der Nutzung einer Technologie oder eines Systems über den ursprünglich vorgesehenen Zweck hinaus verstanden, insbesondere, wenn dies zu einer möglichen Verletzung der Privatsphäre führt.

[9] BGBl. I. Nr. 169/2020 ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2020_I_169/BGBLA_2020_I_169.pdfsig.

[10] oesterreich.gv.at/id-austria.

genau zu verfolgen und möglicherweise notwendige Adaptierungen frühzeitig in einen gesetzlichen Anpassungsprozess einfließen zu lassen. Gleichzeitig erscheint es – insbesondere aus den Erfahrungen mit der CORONA-App lernend – wichtig, alle relevanten Stakeholder frühzeitig in einen möglichst offenen Prozess der Gestaltung einzubinden. Offenheit und Partizipation sind wichtige Pfeiler zukünftiger Akzeptanz derartiger Systeme durch die BürgerInnen.

Vorschlag weiteres Vorgehen

Prozessbegleitung und breiter gesellschaftlicher Diskurs

In einer Überblicksstudie können internationale Lösungen vorgestellt und diskutiert werden sowie der technisch-politische Prozess auf EU-Ebene begleitet und für die Akteure in Österreich nutzbar gemacht werden. Darüber könnte im Rahmen einer Studie eine Klärung grundsätzlicher technischer und sozialer (Privacy-by-)Design-Optionen erarbeitet sowie parallel dazu ein breiter gesellschaftlicher Diskurs organisiert werden – mit dem Ziel, eine akzeptierte österreichische Variante der europäischen eID einzuführen.

Zitierte Literatur

BVerfGE, 1983, BVerfGE 65, 1 – Volkszählung, Urteil des 1. Senats vom 15.12.1983 auf die mündliche Verhandlung vom 18./19.10. 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, oefre.unibe.ch/law/dfr/bv065001.html auch datenschutz-berlin.de/gesetze/sonstige/volksz.htm.

Cater, L., 2021, The EU has introduced a new ‘digital’ ID. Here’s what it means for you., *Politico,* politico.eu/article/eu-europe-digital-id/.

Engemann, C., 2015, E-Identity: Wer garantiert das digitale Ich?, *Zukunftsinstiitut,* zukunftsinstitut.de/artikel/e-identity-wer-garantiert-das-digitale-ich/.

Johnson, M. und Campbell, E., 2020, Biometrics, refugees, and the Middle East: Better data collection for a more just future: Middle East Institute, mei.edu/publications/biometrics-refugees-and-middle-east-better-data-collection-more-just-future.

Kruchem, T., 2020, Leben in der überwachten Gesellschaft, *Deutschalndfunk Kultur,* deutschlandfunkkultur.de/digitale-identitaet-leben-in-der-ueberwachten-gesellschaft.976.de.html?dram:article_id=486012.

Lomas, N., 2021, Europe wants to go its own way on digital identity, *TC,* techcrunch.com/2021/06/03/europe-wants-to-go-its-own-way-on-digital-identity/.

Lutz, R., 2020, Digitale Ausweise – ein Traum für den Überwachungsstaat infosperber.ch/politik/welt/digitale-ausweise-ein-traum-fuer-den-ueberwachungsstaat/.

Schaber, F., Strauß, S. und Peissl, W. (ITA), 2020, *Der Körper als Schlüssel? – Biometrische Methoden für Konsument*innen*, November 2020, Wien: Institut fürTechnikfolgen-Abschätzung, epub.oeaw.ac.at/ita/ita-projektberichte/2020-03.pdf.

Strauß, S., 2019, *Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment*, Abingdon/New York: Routledge.

Wagner, E., 2020, Über Impfstoffe zur digitalen Identität?, *Telepolis*: Heise, heise.de/tp/features/Ueber-Impfstoffe-zur-digitalen-Identitaet-4713041.html?seite=all.