Der Staat kann IT

Der Bund ist bei grossen IT-Projekten immer wieder gescheitert. Im zweiten Anlauf für eine elektronische ID hat er erstmals alles richtig gemacht. Oder fast alles.

Von Adrienne Fichter, 16.04.2024

Der Staat kann IT nicht.

Im Frühjahr 2021 hatte der Bundesrat noch viele Minderwertigkeitskomplexe in Sachen Digitalisierung. Die damalige Justizministerin Karin Keller-Sutter erklärte bei jeder Gelegenheit, dass die Bundesverwaltung unfähig sei, einen staatlichen digitalen Ausweis für ihre Bürger herauszugeben.

Die Herausgabe einer elektronischen ID, einer E-ID, sollte deshalb an zertifizierte private Unternehmen ausgelagert werden. Nach langem Hin und Her entstand ein kompliziertes Gesetz mit mehr als 30 Artikeln. Ein No-Go für die Zivilgesellschaft, die erfolgreich das Referendum ergriff.

So kam es im März 2021 zur Volksabstimmung – und das vom Bundesrat vorgeschlagene privatisierte E-ID-Modell fuhr eine deutliche Niederlage ein. Insgesamt 64 Prozent der Stimmberechtigten lehnten die Vorlage ab. Das Argument der staatlichen IT-Unfähigkeit wollte eine Mehrheit der Stimmbevölkerung nicht gelten lassen. Das Verdikt lautete vielmehr: Der Staat muss IT können. Schweizer Bürgerinnen wollen eine digitale Identitätskarte, die vom Staat ausgestellt wird – analog zum Pass.

Die Gewinner der Abstimmung ruhten sich nicht auf dem Sieg aus, sondern wirkten am zweiten Anlauf für eine E-ID mit. So arbeitete die Digitale Gesellschaft – federführend beim Referendum – gemeinsam mit Nationalrätinnen sechs gleichlautende Motionen aus. Die Digitalpolitiker Min Li Marti (SP), Jörg Mäder (GLP), Gerhard Andrey (Grüne), Franz Grüter (SVP), Simon Stadler (Mitte) sowie die FDP-Fraktion reichten am Mittwoch nach dem Abstimmungssonntag den Vorstoss «Vertrauenswürdige staatliche E-ID» ein. Die politische Stossrichtung für den zweiten Anlauf war damit klar: Die neue E-ID muss vom Staat herausgegeben werden und maximalen Datenschutz für den Bürger bieten.

Das Eidgenössische Justiz- und Polizeidepartement (EJPD) startete daraufhin einen zweiten Anlauf zur E-ID und präsentierte nach drei Jahren das neue Modell: Die Bürgerinnen sollen ab 2026 über eine digitale Brieftasche verfügen, mit der sie sich im Internet ausweisen oder Dokumente unterschreiben können. Das Fedpol soll den Lead bei der Ausstellung und Prüfung der staatlichen Identität haben, das Bundesamt für Informatik und Telekommunikation die IT-Infrastruktur betreiben.

Wer den Prozess mitverfolgt hat, stellte fest: Der Bund machte bei der E-ID-2.0 einiges richtig. Im Folgenden listen wir die wichtigsten Erfolgsfaktoren auf – und erklären, wieso diese zwingend auch für weitere Digitalprojekte des Bundes angewendet werden sollten.

1. Partizipation der Zivilgesellschaft

Das katastrophale Abstimmungsergebnis von März 2021 war ein Beleg dafür, wie sehr sich Bundesbehörden und bürgerliche Politiker irrten. Sie setzten auf ein Modell, das auf die grösstmögliche Akzeptanz bei Schweizer Unternehmen und nicht auf die Bedürfnisse der Bürgerinnen ausgerichtet war.

Das Abstimmungsresultat gab aber auch Aufschluss über die Fehler im Gesetzgebungsprozess. So hatten die Befürworter die Bedenken zum Datenschutz nicht ernst genommen und Warnhinweise der Zivilgesellschaft ignoriert. Die Republik zeichnete in einer Recherche nach, wie die Behörden auch die Vorschläge der Wissenschaft übergingen und wie das Justizdepartement hinter verschlossenen Türen mit dem Unternehmen Swiss Sign den Gesetzestext verhandelte.

Ein fataler Fehler, den man nicht wiederholen wollte. Das Justizdepartement – zuerst unter Karin Keller-Sutter (FDP), dann unter Elisabeth Baume-Schneider (SP) und schliesslich unter Beat Jans (SP) – änderte den Prozess für die zweite E-ID von Grund auf. So haben seit Anfang 2022 fast 20 Partizipationsmeetings stattgefunden, bei denen interessierte Bürgerinnen, Fachpersonen oder Wissenschaftler virtuell oder auch teilweise vor Ort teilnehmen konnten.

Jede Person mit Internetanschluss hatte die Möglichkeit, Kritikpunkte und Vorschläge anzubringen. Die Teilnehmerinnen diskutierten dabei die Grundsatzfragen, die man bei der E-ID-1.0-Debatte nicht stellte: etwa wofür genau eine staatliche E-ID nötig ist, was die konkreten «Use Cases» im Alltag eines Schweizer Einwohners sind und weshalb ein staatlicher digitaler Ausweis nicht dasselbe ist wie bekannte Login-Lösungen (Swiss ID oder eine Google-ID).

Der vom EJPD vorgegebene partizipative Rahmen ermöglichte ein Novum: ein offenes Brainstorming von Gesellschaft, Wissenschaft und Wirtschaft zur Gestaltung einer staatlichen E-ID-Technologie.

Dazu kam: Für die breite Abstützung der E-ID 2.0 führte das EJPD nicht nur ein klassisches Vernehmlassungsverfahren zum Gesetz durch, sondern bot auch zwei Konsultationsverfahren zur Wahl der Technik an: In Letzterem haben die Teilnehmenden die Technologieentscheidung (also ob die digitale Brieftasche eine App sein wird und welche Kryptografie verwendet wird) mit allen Vor- und Nachteilen verhandelt. Ein smarter Move, denn nur so gewinnen Bevölkerung und Fach-Community das notwendige Vertrauen, um eine staatliche E-ID-Lösung überhaupt zu beantragen.

2. Transparenz und Fehlerkultur

Die E-ID-Projektleitung des Bundes hat die technische Dokumentation sowie den Code zu einer potenziell künftigen E-ID-Architektur offengelegt, und zwar auf der Entwicklerplattform Github. Die verschiedenen Rollen des neuen Modells können damit in einem geschützten Raum ausprobiert werden. Also die Bürgerin, die eine E-ID bestellt; der Staat, der diese ausstellt, und die Unternehmen oder Institutionen, die die Daten abfragen werden.

Der Föderalismus dient hierbei nicht als Bremse, sondern als Labor. So testen die Kantone Appenzell Ausserrhoden und Thurgau in Pilotprojekten (ein E-Lernfahrausweis und ein digitaler Kulturausweis) gerade eine solche

digitale Brieftasche. Nicht zuletzt ist später ein Hackerprogramm zur Suche nach Sicherheitslücken (und mit Entschädigung) vorgesehen, wie dies bereits beim E-Voting-System der Post der Fall war.

Die Verantwortlichen setzen also auf maximale Transparenz und testen zu jedem Zeitpunkt die technische Machbarkeit. Auch wischen sie dieses Mal Datenschutzbedenken nicht mehr einfach so vom Tisch.

Nach der Vernehmlassung zur zweiten E-ID-Vorlage im Jahr 2022 gab es von der Digitalen Gesellschaft und der Piratenpartei zwei grosse Kritikpunkte: erstens die Überidentifikation, also dass Firmen bei jeder Gelegenheit Daten verlangen, die sie gar nicht benötigen. Und zweitens die Beantragung einer staatlichen E-ID im missbrauchsanfälligen Videoverfahren. Der deutsche Chaos Computer Club und der Security-Forscher Martin Tschirsich haben vor bald zwei Jahren gezeigt, wie Video-Identifikationsverfahren überlistet werden können und damit auch Identitätsdiebstahl möglich ist.

Das EJPD sowie später auch die zuständige Kommission im Nationalrat haben sich mit den Bedenken auseinandergesetzt – und das Gesetz verbessert: Nun werden Firmen, die zu viele Daten von einer Konsumentin verlangen, sozusagen geoutet. Unklar ist zum jetzigen Zeitpunkt, wie dieses «Outing» genau aussehen soll und wer das in letzter Instanz beurteilen wird. Möglich wäre ein Label (mit der Farbe Rot), das gleich neben dem Unternehmensnamen in einer App angezeigt wird. Die Firma wird damit symbolisch als «datengierig» gebrandmarkt. Der potenzielle Reputationsschaden soll eine abschreckende Wirkung entfalten.

Ausserdem soll jede Bürgerin die Möglichkeit haben, ihre staatliche digitale Identität offline in einem Passbüro vor Ort zu beantragen. Damit fallen auch die Risiken der Videoverfahren beim Fedpol weg.

3. Potenzial zur EU-Kompatibilität

Bei der ersten E-ID-Vorlage hatten die Befürworterinnen behauptet, es gäbe europaweit eine Vielzahl an privaten E-ID-Modellen. Doch dem war nicht so, wie eine Analyse der Republik zeigte. Die meisten EU-Staaten kannten mehrheitlich staatliche E-ID-Lösungen. Wäre das privatisierte und zentralisierte Modell vor drei Jahren an der Urne durchgekommen, so wäre die Schweizer Lösung kaum anschlussfähig an die EU gewesen. Zumal bereits im Jahr 2021 bekannt war, dass die EU mit der E-IDAS-Verordnung eine neue dezentrale IT-Architektur für digitale Identitäten anstrebt.

Dieses Problem hat die Schweiz nun nicht mehr. Denn das E-ID-Modell der Schweiz und der EU ist weitgehend dasselbe, sodass die Schweizer E-ID theoretisch auch bei europäischen Unternehmen und Behörden eingesetzt werden könnte.

Die vollständige Interoperabilität mit der EU ist dieses Mal sogar nicht ganz unproblematisch. Denn sie würde je nachdem sogar Abstriche beim Datenschutz bedeuten, wie das von der E-ID-Projektleitung veröffentliche Diskussionspapier zeigt. Das in der Schweiz derzeit diskutierte Modell fordert strengere Vorgaben. Unternehmen sollten zum Beispiel keine Transaktionen von einzelnen Bürgerinnen anhand von kryptografischen Signaturen miteinander verknüpfen und damit einer Person zuordnen können. Die E-ID-Projektleitung könnte dieses Dilemma technisch gesehen allenfalls mit einer Komponente (Gateway) zwischen den Systemen (Schweiz und EU) lösen.

Zusammengefasst: Die Bundesbehörden haben sich dieses Mal bemüht, kein eigenes Süppchen zu kochen, und arbeiten an einem Kompromiss zwischen EU-Kompatibilität und strengem Datenschutz.

4. Datensparsame Technologiegestaltung

Es ist fast schon ein politisches Mantra in Bundesbern, dass Gesetze zur Digitalisierung «technologieneutral» ausfallen sollen. Das bedeutet: Nicht die Technologien sollen in ein Gesetz geschrieben werden. Sondern deren Auswirkungen müssen mittels Regeln und Verboten reguliert werden. Deswegen existiert bis heute beispielsweise kein spezifisches Schweizer Blockchain-Gesetz.

Dennoch kann der Gesetzgeber Vorgaben zu den Designprinzipien von Technologie machen. Und hier gibt es nun einen entscheidenden Unterschied zur ersten Vorlage. Die Technologiegestaltung liess damals zu viel Raum für kommerzielle Datensammlungen offen. Das heisst: Das alte E-ID-Gesetz hätte ganze Geschäftsmodelle rund um Logindaten erlaubt. Zentralisierte Datenbanken von beauftragten E-ID-Unternehmen wie Swiss Sign wären die Folge gewesen.

Dies ist anders bei der E-ID 2.0, bei der die technologischen Designprinzipien dank der parlamentarischen Vorstösse genau vorgegeben worden sind: Die Hoheit über die Daten liegt in erster Linie bei den Nutzerinnen. Man spricht auch vom Konzept der *self-sovereign identity,* also der selbstbestimmten Verwaltung der eigenen Identität. Der Aussteller der E-ID ist der Staat. Und die Unternehmen sollen nur diejenigen Daten von Konsumentinnen verlangen, die sie wirklich benötigen.

So braucht eine Videoplattform wie Youtube das genaue Geburtsdatum eines Users nicht zu kennen. Sondern dieser muss nur beweisen können, dass er über 18 Jahre alt ist. Verlangt die Videoplattform dennoch das genaue Geburtsdatum und weitere Informationen, so könnte sie das oben erwähnte abschreckende Shaming-Label erhalten.

Fazit: Fast alles richtig gemacht

Nicht alle Fragen rund um die E-ID 2.0 sind heute beantwortet. Offen ist etwa, welche Technologie genau zum Einsatz kommt. Doch jetzt schon gibt es von links bis rechts nur Lob für die neue Vorlage. Ein Referendum scheint eher unwahrscheinlich zu sein.

Und natürlich lässt sich am neuen E-ID-Modell der Schweiz und der EU grundsätzliche Kritik anbringen. Denn die Unternehmen gelangen je nachdem in den Besitz von staatlich verifizierten Daten. Sollten deren Datenbanken wegen schlechter IT-Sicherheit gehackt werden, stehen im schlimmsten Fall sensible und kompromittierende Informationen von Konsumentinnen im Darknet zum Verkauf. Nicht zuletzt wegen solcher Risiken soll die digitale Brieftasche freiwillig sein und nicht verpflichtend.

Die Reaktionen der Bundesbehörden auf die Kritik waren meist souverän – mit einer Ausnahme: Die Ausschreibungsunterlagen für die Anbieterin des Online-Videoverfahrens sind nicht öffentlich auf der Beschaffungsplattform Simap.ch verfügbar. Aus Sicherheitsgründen, sagt das Fedpol. Für Medienschaffende seien die Unterlagen erst nach einem allfälligen Zuschlag öffentlich, erklärt die Beschaffungsbehörde, das Bundesamt für Bauten und Logistik, auf Anfrage der Republik.

Dies sorgt für kritische Reaktionen bei Medien und Bundespolitikern, wie die parlamentarische Frage von SVP-Nationalrat Lukas Reimann zeigt. Im Fachjargon der IT nennt man solche pauschalen Verweise auf die Sicherheit oder Geschäftsgeheimnisse *«security through obscurity»,* was bei einem wichtigen Bestandteil des E-ID-Prozesses – nämlich der Beantragung online beim Fedpol – ein schlechtes Zeichen ist.

Dennoch lässt sich als allgemeines Fazit festhalten: Beim zweiten Anlauf haben die Verantwortlichen nach Massstäben gehandelt, die State of the Art für alle IT-Projekte sein sollten. Das Justizdepartement arbeitete mit der Fach-Community wie bei moderner Softwareentwicklung iterativ, also mit mehreren Feedback-Schlaufen. Und verbesserte damit sukzessive das Ergebnis.

Und wie macht es der Bund anderswo?

Bleibt die Frage: Wie sieht es bei anderen Digitalgesetzen aus? Erfüllen sie die oben geschilderten Benchmarks?

Eine Auswahl von drei aktuellen IT-Projekten und -Regelwerken zeigt ein gemischtes Bild.

Beim Thema KI-Regulierung ist es zwar noch zu früh für ein Urteil. Der Prozess sieht schon mal vielversprechend aus: Das Bundesamt für Kommunikation (Bakom) und das EJPD arbeiten eine Auslegeordnung für die Regulierung von künstlicher Intelligenz aus, die im Herbst 2024 vorliegen soll. Hierbei kann sich jede interessierte Person einbringen bei der Bundesplattform Tripartite, einem offenen Forum für Diskussionen zur Digitalpolitik. Die erste Sitzung fand am 15. April statt, die zweite ist im Juni geplant. Das Bakom bestätigt auf Anfrage: Das Interesse am Forum ist beachtlich.

Ob dieses Forum wie bei der E-ID 2.0 institutionalisiert in den Gesetzgebungsprozess eingebunden wird, lässt sich noch nicht sagen. Natürlich ist eine KI-Regulierung nicht 1:1 vergleichbar mit einer staatlichen digitalen Dienstleistung wie bei der E-ID. Denn bei einem allfälligen KI-Gesetz geht es darum, Regeln für die Wirtschaft und den öffentlichen Sektor im Umgang mit künstlicher Intelligenz zu entwickeln. Doch bei einem derart wichtigen Thema für Wirtschaft und Gesellschaft ist ein inklusiver Prozess umso relevanter. Nur mit einem breit abgestützten Gesetz kann ein Referendum vermieden werden. Auch wird interessant, wo sich die Schweiz im Spannungsfeld zwischen dem Schweizer Ansatz (kein umfassendes KI-Gesetz, sektorale Gesetzesanpassungen) und der EU (ein horizontales KI-Gesetz mit Ausnahmen für die Sicherheitsbehörden) positionieren wird.

Die EU schreibt zudem Eingriffe in die Technik vor, wie etwa die Prüfung von Trainingsdatensätzen bei den grossen Sprachmodellen. Etwas, das in der unternehmensfreundlichen Schweiz kaum denkbar wäre. Die Organisationen Algorithmwatch Schweiz, Digitale Gesellschaft und auch CH++ haben sich schon früh für verbindliche Regularien bei den Anwendungen von KI-Systemen positioniert. Ihre Bedenken zu ignorieren, würde nur den Fehler der E-ID-Befürworter wiederholen.

Eher fragwürdig läuft der aktuelle Prozess bei der Plattformregulierung. Hier tüftelt die Schweiz an einem Äquivalent zum neuen «Digital Services Act» der EU. Es ist eine Art «Durchsetzungsgesetz» für das Zivil- und Strafrecht der europäischen Staaten. Demnach müssen die grossen Big-Tech-Konzerne Beschwerdewege für Nutzerinnen einrichten, ihre Al-

gorithmen erklärbar machen und ihre Plattformen moderieren. Beispielsweise haben sie bei gewaltverherrlichenden Postings einzugreifen. Nur so können Straftatbestände wie Verleumdung und Betrug auf Social Media durch die Strafverfolgung geahndet werden.

Auch die Schweiz will dieses digitalpolitische EU-Gesetz autonom nachvollziehen. Zuerst fanden Anhörungen in der Staatspolitischen Kommission des Nationalrats statt, bei denen Organisationen wie Algorithmwatch Schweiz, aber auch Unternehmen wie Google Schweiz ihre Meinungen darlegen konnten. Doch seither arbeitet das Bakom unter der Federführung des SVP-Bundesrats Albert Rösti hinter verschlossenen Türen an einer Vorlage. Das Bundesamt hatte ursprünglich einen Entwurf für Frühling 2024 angekündigt, verschob diesen Termin aber gemäss Recherchen von «Le Temps» auf Herbst 2024.

Dies geschah, obwohl es sich hier um Themen wie Hassrede und Falschinformationen handelt, bei denen man zwingend auf Impulse der Zivilgesellschaft und der Wissenschaft angewiesen ist. Und bei denen dringend Lösungen nötig sind, wie die Hass-Postings auf Instagram des jugendlichen Attentäters in Zürich zeigten.

Hoffnungslos scheint der Fall beim elektronischen Patientendossier zu sein. Das Mammutprojekt wird wohl auch wegen vieler digitaler Altlasten der Nullerjahre nicht zum Fliegen kommen. Das Patientendossier stammt aus einer Ära mit weniger Fokus auf die Autonomie von Patientinnen – und aus einer Ära, in der sich die digitale Zivilgesellschaft der Schweiz noch in den Kinderschuhen befand.

Auch hat das zuständige Bundesamt für Gesundheit den Technologieentwicklungsprozess weder transparent noch partizipativ geführt: Die Vergabe für die Technologieanbieter durch die Stammgemeinschaften erfolgte unter Ausschluss der Öffentlichkeit. Die Post als wichtigste Technologielieferantin muss bis heute keinen Code präsentieren. Die Zertifizierungen durch die KPMG werden auch auf Medienanfrage nicht rausgegeben. Und das Patientendossier wurde an den Bedürfnissen der Ärztinnen und Spitäler vorbei entwickelt, weswegen bis heute von medizinischer Seite viel Widerstand kommt. Nicht umsonst redet man heute auch von einem «PDF-Friedhof», weil die Daten der Patientinnen weder strukturiert noch maschinenlesbar sind (und damit auch nicht anonymisiert für die Forschung zur Verfügung stehen).

Beim Patientendossier wäre vielleicht dasselbe nötig wie nach der Abstimmungsniederlage bei der E-ID: den Reset-Button drücken, auf Feld eins zurückgehen – und das Projekt entlang der vier aufgeführten Grundsätze neu starten.