Ctrl-Alt-R

Das Märchen vom E-ID-Wettbewerb

Bisher unveröffentlichte Dokumente zur Verordnung über die elektronische Identität zeigen: Egal für welchen Anbieter Sie sich entscheiden – am Schluss weiss jeder alles über Sie.

Von Adrienne Fichter, 09.02.2021

Kürzlich hat die Republik ein wesentliches Problem mit der Schweizer E-ID thematisiert: Die Verordnung zum Gesetz, über das die Schweiz am 7. März abstimmt, ist bisher nicht veröffentlicht. Darin werden technische Grundsätze definiert – mit Folgen für den Datenschutz und die Datensicherheit.

Gestützt auf das Öffentlichkeitsgesetz hat die Republik Zugang zu allen Dokumenten der Arbeitsgruppe verlangt, die in regelmässigen Abständen tagt und den Gesetzgebungsprozess berät. Vertreten sind das Konsortium Swiss Sign, die Stadt Zug, der Kanton Schaffhausen, die Internetorganisation Switch, die Fachorganisation eHealth und die Bundesämter für Polizei und für Justiz.

Das Bundesamt für Justiz hat nun – bemerkenswerterweise – ungeschwärzt alle Präsentationen, Stellungnahmen und E-Mails der Arbeitsgruppe aus dem Zeitraum November 2018 bis August 2020 ausgehändigt. Brisant ist vor allem ein Punkt: der Datentransfer zwischen den E-ID-Anbietern. Im Fachjargon spricht man dabei von «Interoperabilität».

Parlamentarierinnen hatten sich in der Beratung dafür eingesetzt, dass kein Bürger benachteiligt sein soll – unabhängig davon, für welche Lösung er sich entscheidet. So steht nun im E-ID-Gesetz:

> IdP [Identitätsprovider] akzeptieren ihre E-ID-Systeme gegenseitig und stellen sicher, dass die E-ID-Systeme interoperabel sind.

Artikel 18, E-ID-Gesetz.

Was die National- und Ständerätinnen offensichtlich zu wenig bedacht haben, ist, welche technischen Operationen im Hintergrund laufen müssen, damit Interoperabilität gewährleistet ist, und was das für den Datenschutz heisst.

Gestützt auf die Dokumente der Begleitgruppe wird nämlich deutlich: Die Interoperabilität sorgt für einen permanenten Informationsaustausch zwischen den E-ID-Anbietern und macht die Nutzerinnen zu gläsernen Bürgern.

Ein Beispiel: Nehmen wir an, Lena Fischer (Sie erinnern sich vielleicht noch an unsere Musterperson aus dem letzten Text) hat sich eine E-ID des Kantons Schaffhausen ausstellen lassen – von einem der möglicherweise landesweit vorgesehenen Anbieter.

Nun will sie im Kanton Jura wegen ihres Studiums ein Stipendium beantragen. Lena Fischer steuert dazu die E-Government-Website des Kantons Jura an und findet dort eine Benutzermaske – das E-ID-Log-in. Diese Maske ist einheitlich gestaltet, um das Look-and-feel eines staatlichen Passes zu vermitteln. (So steht es in einer Präsentation vom 14. August: «Die Designelemente werden vom Bund vorgegeben.»)

Der Kanton Jura kooperiert jedoch mit dem Unternehmen Swiss Sign-, das die Swiss ID herausgibt, eine andere E-ID. Diese ist bereits heute in die Website Guichet virtuel integriert. Wer etwa ein Stipendium beantragt, kommt aktuell nicht an dieser ID vorbei.

Was passiert nun im Hintergrund, wenn das Gesetz angenommen wird?

Lena Fischer wird auf der E-Government-Website des Kantons Jura eine einheitliche E-ID-Maske antreffen. Sie wird dort aufgefordert, ihren Benutzernamen (zum Beispiel Lena.Fischer@juraID) einzugeben. Obwohl sie beim Anbieter aus Schaffhausen registriert ist, übernimmt Swiss Sign ab diesem Zeitpunkt das Zepter. Der Datenaustausch mit Schaffhausen beginnt.

Swiss Sign wird im Zuge der Anmeldung den Benutzernamen von Lena Fischer erfahren (ein eindeutiges Identifikationsmerkmal), die Kundennummer der besuchten Behörde sowie im Fall des Jura – aufgrund einer fehlerhaften Konfiguration – sogar die genaue Adresse der besuchten Website. Kurz: Swiss Sign erfährt, dass Fischer sich im Jura angemeldet und dort einen Antrag auf finanzielle Unterstützung im Bildungsbereich einreicht. Nicht nur der eigentliche, sondern auch ein fremder Identitätsprovider weiss damit Bescheid über ihr Vorhaben.

Damit wird der viel zitierte «Wettbewerb der besten E-ID-Lösungen» ad absurdum geführt. Unabhängig davon, für welche Lösung sich die Bürgerin entscheidet, und mag sie noch so datenschutzfreundlich sein: Sie wird sich nicht vor «fremden» Anbietern verstecken können.

Konkret: Sie wird ihr Surfverhalten nicht vor dem Platzhirsch, der Swiss-Sign-Gruppe, verbergen können. Ihr Produkt ist bereits heute in die Onlineportale von bald neun Kantonen und zahlreichen Grossunternehmen wie zum Beispiel SBB, Post und Mobiliar integriert. Das beschert Swiss Sign einen Datenstamm von mehreren Millionen Nutzerinnen. Egal, ob es dem Kanton Schaffhausen also gelingen wird, sich als staatliche E-ID zu zertifizieren: Swiss Sign wird sehr vieles über die Internetaktivitäten von Schweizer Bürgerinnen erfahren.

Die Verordnung befindet sich zurzeit in der Phase der Ämterkonsultation; sie zirkuliert also intern in der Bundesverwaltung. Technische Änderungen sind noch möglich. Doch Mitglieder der Begleitgruppe sagen, dass sie sich auf den beschriebenen Modus Operandi in Sachen Interoperabilität einstellen.

Auch das Bundesamt für Justiz bestätigt den skizzierten Ablauf und die Weitergabe der betreffenden Daten. Informationschefin Sonja Margelist betont aber: «Die dabei anfallenden Nutzungsdaten unterstehen den strikten Vorgaben des E-ID-Gesetzes.»

Ich will es genauer wissen: Was ist von der Reaktion der Bundesverwaltung auf die Kritik an der E-ID zu halten?

Das Thema Datenschutz scheint die Bundesverwaltung immer mehr in Erklärnot zu bringen. Einen Tag nach Veröffentlichung des Beitrags über die Probleme mit der Schweizer E-ID in der Republik publizierte das Bundesamt für Justiz eine Auslegeordnung. Vieles davon nahm Bezug auf die Kritikpunkte, ohne diese zu entkräften. Darunter sind einige fragwürdige Interpretationen des eigenen Gesetzes.

Das Bundesamt schreibt etwa, dass erstmals «Datenschutz by Design» in einem Gesetz verankert werde, weil die E-ID-Anbieter die Identitätsdaten (den Namen und das Geburtsdatum von Lena Fischer) getrennt von den Nutzungsdaten (Surfen bei Galaxus) speichern müssen. Doch diese Trennung hat wenig mit dem Prinzip «Privacy by Design» zu tun. Denn auch hier ist man auf den Goodwill der Identitätsprovider angewiesen. Es ist keine Architektur vorgeschrieben, die Datensparsamkeit und Datenhoheit bei Nutzerinnen zur Pflicht erklärt.

Ausserdem wird diese Trennung bei jedem Einloggen ständig aufgehoben. «Egal, wie die physische Trennung der Daten ist, zur Laufzeit müssen alle Speicherorte zusammenarbeiten, und es gibt Links, die die Daten zusammenhalten», sagt Annett Laube, Informatikprofessorin an der Berner Fachhochschule.