E-ID Gesetz & Datenschutz

Von RA lic. jur. Ursula Sury

Ausgangslage

In der Herbstsession 2019 hat das Parlament das Bundesgesetz über elektronische Identifizierungsdienste (BGEID oder E-ID-Gesetz) verabschiedet. Damit soll die Handhabung elektronischer Identitäten (E-ID) geregelt werden.

Die elektronische Identität soll das Leben der Internetnutzerinnen und -nutzer in der Schweiz einfacher machen. Mit einem einzigen Login können sie sich auf den unterschiedlichsten Websites anmelden. Vergessene Passwörter sollen der Vergangenheit angehören. Doch die E-ID kann noch mehr, sie kann auch die Identität oder das Geburtsdatum der Nutzenden nachweisen. Damit lässt sich zum Beispiel online ein Arzttermin vereinbaren, eine Behörde kontaktieren oder ein Whisky kaufen. Die staatlich anerkannte E-ID soll dabei garantieren, dass niemand Missbrauch betreibt oder sich als andere Person ausgibt. Wer im Internet Waren oder Dienstleistungen bezieht, muss sich identifizieren. Dafür gibt es verschiedene Verfahren, oft mit Benutzername und Passwort. Aber keines dieser Verfahren ist in der Schweiz gesetzlich geregelt und für keines übernimmt der Bund eine Garantie, wonach es sicher und zuverlässig funktioniere.

Wie wird die E-ID angewendet?

Die Verwendung einer E-ID ist freiwillig. Wer eine nutzen will, stellt zuerst bei einer vom Bund anerkannten E-ID-Anbieterin einen Antrag. Die Anbieterin übermittelt den Antrag an den Bund, der die Identität der antragstellenden Person prüft und der Anbieterin grünes Licht für die Ausstellung der E-ID gibt. Bund und Parlament gehen davon aus, dass es mehrere Anbieterinnen geben wird, die miteinander im Wettbewerb stehen. Es ist möglich, sich bei mehreren Identity-Providern gleichzeitig anzumelden.

Das E-ID-Gesetz legt fest, dass der Staat die Hoheit über den Identifizierungsprozess behält. Wie beim Pass oder der Identitätskarte, die durch akkreditierte Unternehmen hergestellt werden, ist der Staat weiterhin für die amtliche Bestätigung einer Identität zuständig. Die technische Infrastruktur hingegen wird von privaten Unternehmen entwickelt und betrieben. Diese Aufgabenteilung ist zweckmässig. Indem das bestehende Know-how von Schweizer Unternehmen genutzt wird, lässt sich die E-ID rasch umsetzen, ohne dass die Kontrollfunktion des Staates geschwächt oder hoheitliche Rechte beschränkt werden. Der Bund reguliert und kontrolliert die Anbieter von E-ID-Lösungen. Um sich als sogenannter Identity-Provider zertifizieren zu können, müssen Unternehmen eine Reihe von Kriterien erfüllen. Auch müssen die Daten in der Schweiz gespeichert und bearbeitet werden.

Nicht nur für die Bürger, auch bei den Behörden führt das neue Gesetz zu Vereinfachungen. So hängt zum Beispiel die erfolgreiche Einführung des elektronischen Patientendossiers oder eine medienbruchfreie digitale Steuererklärung massgebend von einer sicheren und damit akzeptierten elektronischen Identität ab. Die Kantone und Gemeinden sind noch stärker als der Bund auf den direkten Kontakt mit den Bürgern ausgerichtet und daher in besonderem Masse an einer E-ID-Lösung interessiert. Zudem zeigt die aktuelle Coronakrise, dass eine verlässliche E-ID einen wichtigen Beitrag zur Reduktion von Behördengängen einzig zum Zweck der Unterzeichnung leisten kann. Solche Vereinfachungen haben letztlich auch einen positiven Effekt auf die kantonalen Finanzen.

Datenschutzrechtliche Risiken

Bei der Ausstellung und der Nutzung der E-ID können, wie bei jedem Identifizierungsverfahren, sensible Daten der Userinnen und User missbräuchlich verwendet werden. Im Folgenden werden einige Risiken aufgezeigt, welche sich insbesondere bezüglich des Datenschutzes ergeben können.

Mit dem E-ID-Gesetz besteht ein Risiko, dass die Datenweitergabe seitens der E-ID-verwendenden Dienste, insbesondere innerhalb eines Konzerns nicht genau geregelt wird. Wohl definiert das Datenschutzgesetz in Art. 4 Abs. 3 den Grundsatz der Zweckbindung und die Tatsache, dass der Verwendungszweck der Datenbeschaffung feststehen und ersichtlich sein muss, jedoch kann dies aber mittels Datenschutzerklärung bei der Erstregistrierung relativ einfach umgangen werden.

In den Privacy-Statements könnten dann Aussagen wie: «Die Einwilligung zur Datenweitergabe innerhalb des Konzerns zwecks Verbesserung der eigenen Produkte wird erteilt» oder «Der Verwendung der persönlichen Daten zur Steigerung der Nutzererfahrung innerhalb des Konzerns wird zugestimmt.» Gerade Letzteres wird meistens dazu benutzt, Datenauswertungen zu erstellen, um beispielsweise die Suchergebnisse zu verfeinern.

Das E-ID-Gesetz macht des Weiteren keine Aussagen darüber, ob Daten in der Cloud gespeichert werden dürfen, wenn die Betreiberin von hinreichenden Schutzgarantien durch Verträge im Ausland ausgeht (Art 6. Abs. 2 lit a. DSG).

Datenschutzrechtliche Chancen

Die datenschutzrechtlichen Vorteile der selbstbestimmten Identität auf der Blockchain sind demgegenüber vielversprechend. Die Datensicherheit ist gewährleistet und unzulässige Zugriffe auf die Daten werden erschwert bis verunmöglicht. Die Zugriffe erfolgen transparent und können dadurch rückverfolgt werden. Die Daten fliessen zudem nur in einem begrenzten Masse, da der Nutzende die Menge kontrollieren kann. Dies kommt dem Verhältnismässigkeits-Prinzip der Datenbearbeitung zugute, wonach nur die für einen bestimmten Zweck erforderlichen Daten bearbeitet werden sollen. Die Daten sind zudem vor Verfälschungen geschützt, da für eine Änderung oder eine Löschung der Daten die Zustimmung nötig wäre. Nicht zu vergessen ist u.a. auch die Datenportabilität. Der Benutzer erhält dadurch die Möglichkeit seine personenbezogenen Daten bei einem Anbieterwechsel mitzunehmen, was das Recht des Einzelnen auf informationelle Selbstbestimmung stärkt. Auch aus Sicht der Online-Anbieterinnen gibt es einen wichtigen Vorteil zu nennen. Bisher bestand eine gewisse Unsicherheit darüber, ob eingeloggte Nutzende auch tatsächlich Eigentümerinnen resp. Eigentümer der Logindaten sind. Die SSI-Zertifikate werden beim SSI-Modell ausschliesslich der berechtigten Person zugeteilt und in deren «Wallet» gespeichert, sodass nur die jeweilige Eigentümerin/der jeweilige Eigentümer sie verwenden kann. Durch die SSI lassen sich Nutzende somit unverfälscht identifizieren.

Fazit

Mit einem Reisepass oder einer Identitätskarte kann eine Person ihre Identität im Alltag beweisen. Im Internet ist dieser Beweis derzeit nur sehr umständlich zu erbringen. Daher braucht es für die digitale Welt einen elektronischen Identitätsnachweis, auch E-ID genannt. Solche staatlich anerkannten elektronischen Identifizierungsmittel sind für die weitere Entwicklung von Online-Geschäften und E-Government-Anwendungen wichtig.

E-ID Anbieterinnen könnten jedoch personenbezogene Daten der Nutzenden speichern und auswerten. Der Persönlichkeitsschutz der Nutzenden würde dadurch tangiert werden und muss daher zweckgebunden geschützt werden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und Vizedirektorin an der Hochschule Luzern – Informatik. Sie ist zudem Dozentin für Informatikrecht in verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.