

Ausführliches Argumentarium

Inhaltsverzeichnis

E-ID: Fraglicher Zweck.....	2
Datenspuren im Alltag.....	3
Keine Garantien.....	4
Fehlende Freiwilligkeit.....	5
Keine Transparenz.....	6
E-ID-Daten fließen an Big Tech.....	7
KI: erhöhte Gefahr.....	8
Cyberangriffe.....	9
Gefährlichkeit von Massenüberwachung.....	10
Haftungsrisiken.....	11
Sozialkreditsystem.....	12

E-ID: Fraglicher Zweck

Die E-ID wird im entsprechenden Gesetz lediglich als “elektronischer Identitätsnachweis” beschrieben¹. Was dies genau bedeutet, erklärt der Bund nicht. Die E-ID ist damit im Grundsatz eine Blackbox.

Es werden zwei Verwendungszwecke angeführt: Einerseits Behördengänge², für welche es bereits das Behörden-Login³ gibt. Andererseits die Altersverifikation im Alltag⁴, etwa am Kiosk. Dafür ist die normale Identitätskarte besser geeignet, weil keine Daten gespeichert werden. Die bisherigen Ausweise sind der E-ID in beiden Punkten — Datensparsamkeit und Sicherheit⁵ — überlegen. Am deutlichsten wird die E-ID definiert durch die vorgesehene Kompatibilität mit der EU⁶. Wer wissen will, was die E-ID der Schweiz werden soll, muss deshalb die Entwicklungen der Gesetze und technischen Standards der EU verfolgen. Diese ändern stetig und sind deshalb weitgehend ungewiss. Der Bundesrat verschafft sich im E-ID-Gesetz deshalb die Kompetenz selbständig über die Gestaltung der E-ID zu entscheiden, das bedeutet für die Bevölkerung eine grosse Unsicherheit.⁷

¹ Art. 1, Abs. 2 c, BGEID; https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_1

² Botschaft zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise, 22. November 2023; PDF; S.2; <https://www.fedlex.admin.ch/eli/fga/2023/2842/de>;

³ Behörden-Login; <https://www.agov.admin.ch/de> und <https://www.digitale-verwaltung-schweiz.ch/umsetzungsplan/agenda-dvs/potenzial-zur-automatisierung-und-vereinfachung-fuer-die-wirtschaft-ausschoepfen>

⁴ Botschaft zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise, 22. November 2023; PDF; S.2; <https://www.fedlex.admin.ch/eli/fga/2023/2842/de>;

⁵ Prinzip der Datensparsamkeit https://de.wikipedia.org/wiki/Datenvermeidung_und_Datensparsamkeit

⁶ Zitat: “In jedem Fall hält das Schweizer E-ID-System internationale Standards ein, damit die E-ID dereinst auch im Ausland anerkannt und eingesetzt werden kann.”; PDF; S.2; URL: <https://www.fedlex.admin.ch/eli/fga/2023/2842/de>

⁷ Art. 32, BGEID; https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_32

Datenspuren im Alltag

Bislang gilt für uns Bürger und Bürgerinnen im digitalen Raum und auch im Alltag⁸: Pass und ID werden kaum verlangt und auch nicht gespeichert. Es fallen bisher wenig bis keine Daten an. Die E-ID ändert dies: sie fördert, dass ständig und unnötig⁹ personenbezogene Daten¹⁰ gespeichert werden. Darunter Namen, Geburtsdaten, die AHV-Nummern und biometrische Gesichtsbilder, die dann Zielscheibe von Angriffen¹¹ und Analysen werden können. Das ist ein unnötiges Sicherheitsrisiko.

⁸ [https://de.wikipedia.org/wiki/Identit%C3%A4tskarte_\(Schweiz\)](https://de.wikipedia.org/wiki/Identit%C3%A4tskarte_(Schweiz))

⁹ Art. 23, Abs. 1 & 2, BGEID; https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_23

¹⁰ Art. 15 Abs. 1 & 2, BGEID; https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_15

¹¹ Cybervorfälle Schweiz; <https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html>

Keine Garantien

Das E-ID-Gesetz bietet keine sicheren Datenschutz-Standards. Es benutzt zwar Schlagwörter aus der Datenschutz-Sprache, garantiert aber nichts. Unternehmen können mittels der E-ID beliebig Daten sammeln, verknüpfen¹², analysieren und daraus Verhaltensprofile der Bürgerinnen und Bürger anfertigen. Diese können für Werbezwecke oder politische Beeinflussung benutzt werden.¹³

¹² Stand Heute "selective disclosure" S. 7 – 13 https://c4dt.epfl.ch/wp-content/uploads/2024/11/E-ID_slides_summary.pdf

¹³ <https://www.nature.com/articles/s41562-022-01460-1>

Fehlende Freiwilligkeit

Im Gesetz fehlt der Grundsatz, dass die E-ID freiwillig bleiben wird: Extrakosten¹⁴ für Dienstleistungen ohne E-ID drängen die Bevölkerung zur Nutzung. Menschen mit wenig Geld, ältere Personen oder andere Gruppen, die eine Nutzung nicht wollen oder sich nicht leisten können, werden benachteiligt.

¹⁴ Art. 31 Abs. 4, BGEID https://www.fedlex.admin.ch/eli/fga/2025/20/de/art_31

Keine Transparenz

Die E-ID befolgt den Grundsatz der Transparenz¹⁵ nicht: die Software ist nicht vollständig open-source. Das Gesetz bietet Schlupflöcher, wodurch der Bund die Möglichkeit hat, sich einer Offenlegung der Technologie zu entziehen¹⁶. Das ist bei einem staatlichen Projekt inakzeptabel. Entscheidende Teile der Technologie — namentlich das Online-Ausstellungsverfahren — werden bereits jetzt geheim gehalten und entziehen sich unabhängigen Sicherheitsprüfungen und damit der demokratischen Kontrolle.

¹⁵ Art. 12 Abs. 2, BGEID https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_12

¹⁶ Art. 18 Abs. 6, BGEID https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_18

E-ID-Daten fließen an Big Tech

Ein mit der E-ID inhaltlich verbundenes Gesetz¹⁷ verlangt, dass alle Bürgerinnen und Bürger in Zukunft bei der Benutzung von Social Media ihre Identitäts-Daten an Big Tech¹⁸ liefern müssen. Dies ist besonders heikel, da auf Social Media detaillierte, psychologische Verhaltensprofile von allen Menschen angefertigt werden. Diese Verhaltensprofile können dann mit den Schweizer Pass-Daten verbunden werden. Im Fall von TikTok fließen unsere Verhaltensprofile mit den damit verbundenen Schweizer Pass-Daten an den chinesischen Staat.

¹⁷ <https://www.bsv.admin.ch/bsv/de/home/sozialpolitische-themen/kinder-und-jugendfragen/jugendschutz/jugendschutz-bei-filmen-und-videospielen.html>

¹⁸ <https://taz.de/Lobbyismus-von-Digitalkonzernen/!6058775/>

KI: erhöhte Gefahr

Komplexe Algorithmen der künstlichen Intelligenz schaffen neue Möglichkeiten zur Datenauswertung (Deep Data Mining) und ermöglichen die Analyse der Menschen in bisher unbekanntem Ausmass. Auch vereinfacht KI die Ausführung von Cyberangriffen¹⁹ – und damit die Wahrscheinlichkeit von kriminellen Zugriff auf unsere Daten, siehe ‚Cyberangriffe‘.

¹⁹ https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240430_Paper_Einfluss_KI_Cyberbedrohungslage.html

Cyberangriffe

Bei jedem Gebrauch der E-ID speichern Firmen sensible²⁰ Pass-Daten auf ihren Servern. Viele Firmen verfügen nicht über ausreichende Cyber-Sicherheits-Systeme. Somit sind Unternehmen und die Daten von uns Bürgerinnen und Bürgern ein leichtes Ziel für kriminelle Hacker. Das E-ID-Gesetz müsste von den Unternehmen deshalb zusätzliche Sicherheitsstandards verlangen und deren Einhaltung regelmässig prüfen.

²⁰ <https://www.srf.ch/news/wirtschaft/cybersicherheit-in-spitaelern-schweizer-spitaeler-innert-stunden-gehackt> , <https://www.republik.ch/2021/03/23/wollen-sie-wissen-womit-viola-amherd-geimpft-ist> , <https://www.srf.ch/news/schweiz/swisstransplant-enorme-sicherheitsmaengel-im-organspende-register> , <https://www.tagesanzeiger.ch/vw-22000-kunden-in-der-schweiz-von-datenleck-betroffen-371474996353>

Gefährlichkeit von Massenüberwachung

Überwachung²¹ kann sowohl von privaten Unternehmen als auch von staatlichen Institutionen²² ausgehen. Private Unternehmen verkaufen die Daten aus dieser Überwachung für finanzielle Gewinne. Staaten können sie einsetzen, um ihre Bürgerinnen und Bürger zu analysieren und kontrollieren.

Beide Formen der Überwachung stehen im Widerspruch zu den Prinzipien demokratischer Systeme und haben das Potenzial, diese zu untergraben. Überwachung betrifft daher nicht nur das Individuum, sondern ihre Gefährlichkeit erstreckt sich auf die gesamte Gesellschaft. Überwachung hat weitreichende Konsequenzen für die demokratische Ordnung – und damit für zukünftige Generationen.

²¹ <https://www.bpb.de/themen/medien-journalismus/netzdebatte/169173/das-kontrollierte-selbst-warum-ueberwachung-uns-allen-schadet/> , <https://www.amnesty.ch/de/themen/ueberwachung/zahlen-fakten-und-hintergruende>

²² <https://www.republik.ch/2024/01/09/der-bund-ueberwacht-uns-alle>

Haftungsrisiken

Bürgerinnen und Bürger haften selbst für die Sicherheit ihrer E-ID im Missbrauchsfall. Dies ist bei bisherigen Ausweisdokumenten nicht der Fall. Was diese Haftung im Detail und Einzelfall bedeutet, ist unklar.²³

²³ Art. 22 Abs. 1 + 2, BGEID https://www.fedlex.admin.ch/eli/fga/2025/20/de/art_22

Sozialkreditsystem

Die Infrastruktur der E-ID wird an einigen Orten auf der Welt zur Überwachung und Kontrolle der Bevölkerung verwendet, namentlich mit Sozialkreditsystemen²⁴. Diese bewerten Bürgerinnen und Bürger nach einem Punktesystem. Der bekannteste Fall ist China. Aber auch in Österreich und Italien sind ähnliche Systeme im Test. Diese sind gefährlich für die Menschen und widersprechen der Demokratie im Grundsatz. Damit eine E-ID in Zukunft sicher sein kann und das Vertrauen der Bevölkerung hat, muss der Betrieb von Sozialkreditsystemen durch das E-ID-Gesetz verboten werden. Prinzipiell ist ein Verbot von Sozialkreditsystemen auch in der Bundesverfassung notwendig.

²⁴ <https://www.infosperber.ch/freiheit-recht/datenschutz/chinas-sozialkredit-system-kommt-schleichend-auch-bei-uns/>