



Dienstag, 23. September 2025, 16:00 Uhr
~11 Minuten Lesezeit

Der digitale Fichenstaat

Der neue Entwurf für das E-ID-Gesetz in der Schweiz gibt vor, Datenschutz und Freiwilligkeit zu beachten und ist dennoch eine Mogelpackung — am 28. September entscheiden die Bürger an der Urne.

von Michael Straumann
Foto: Kitinut Jinapuck/Shutterstock.com

Es war Ende der 1980er Jahre, als nach Kontroversen

um die Bundesrätin Elisabeth Kopp ans Licht kam, dass die schweizerischen Behörden fast ein Jahrhundert lang Informationen über die eigenen Bürger gesammelt und in Karteikarten, sogenannten Fichen, fein säuberlich archiviert hatte. Der Fichenskandal liegt mittlerweile 35 Jahre zurück und hat sich doch eingebrannt ins schweizerische Verständnis von Datenschutz. Nun verleiht die digitale Identität der Diskussion um staatliche Überwachung eine neue Dimension. Die hierdurch gesammelten Daten lassen keinen riesigen Raum mit deckenhohen Regalen entstehen, sie sind unsichtbar, aber dennoch sind sie da. 2021 wurde der erste Entwurf des Bundesrates für ein E-ID-Gesetz vom Wahlvolk abgelehnt. Jetzt steht einer neuer zur Abstimmung, in einigen Punkten verändert, jedoch genauso gefährlich.

Weltweit gewinnt die digitale Identität an Boden. Die EU arbeitet an einer Altersverifikations-App

(https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1820), die die E-ID direkt mit den Online-Aktivitäten der Bürger verknüpfen soll. Der Prototyp

(<https://www.techradar.com/computing/cyber-security/after-the-uk-online-age-verification-is-landing-in-the-eu>) läuft bereits in Italien, Dänemark, Spanien und Griechenland. Parallel dazu wird eine digitale Briefftasche

(https://web.archive.org/web/20250214112039/https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de) entwickelt, in der künftig Führerschein, Gesundheitsdaten und Bankkarten Platz finden.

Auch Deutschland treibt die elektronische Identität voran: Der Koalitionsvertrag

<https://web.archive.org/web/20250414132558/https://www.wiwo.de/downloads/30290756/7/koalitionsvertrag-2025.pdf>) **der schwarz-roten Regierung sieht ein verpflichtendes Bürgerkonto und eine E-ID vor, die mit der EU-Brieftasche gekoppelt wird. Im Vereinigten Königreich ist die elektronische Identität schon heute Voraussetzung für Arbeitsplatz, Wohnung und Gesundheitsversorgung.**

Australien geht noch weiter: Dort soll der Zugriff auf Internetsuchmaschinen wie Google oder Bing künftig nur noch mit E-ID möglich sein. In Schweden gilt sie zwar offiziell als freiwillig, ist aber im Alltag faktisch **unverzichtbar**

<https://www.youtube.com/watch?v=6ZgAxr9ikkk&t=113s>) – sei es bei Bankgeschäften, Steuererklärungen oder Arztbesuchen.

Österreich wiederum setzt auf Druck: Wer die staatliche **ID Austria** (<https://www.id-austria.gv.at/de/verwenden/app-id-austria>) verweigert, kann sanktioniert werden. So **verlor** (<https://www.derstandard.at/story/3000000279827/lehrerin-weigerte-sich-id-austria-zu-verwenden-und-wurde-gekuendigt-was-steckt-dahinter>) kürzlich eine Lehrerin ihre Stelle, weil sie sich weigerte, die digitale Identität zu nutzen.

Auch in der Schweiz drängt die Politik auf eine E-ID – gebremst einzig durch die direkte Demokratie. 2021 lehnte das Stimmvolk die damalige **Vorlage** (https://de.wikipedia.org/wiki/Eidgen%C3%B6ssische_Volksabstimmung_%C3%BCber_das_E-ID-Gesetz) mit deutlichen 64,4 Prozent ab. Statt diesen Entscheid zu akzeptieren, legte der Bundesrat rasch nach: In der neuen Gesetzesvorlage soll der digitale Identitätsnachweis nicht mehr von privaten Firmen, sondern angeblich vom Staat herausgegeben werden. Doch auch dieses Gesetz kommt glücklicherweise vors Volk. Am 28. September entscheidet sich, ob die Bürger die E-ID erneut ablehnen – oder ob

sie sich diesmal von den Versprechen des Bundesrats und seiner Befürworter überzeugen lassen.

Alles andere als staatlich

Offiziell begründet der Bundesrat seinen neuen Anlauf mit dem Argument, die erste Vorlage sei am Widerstand gegen private

Herausgeber

(<https://x.com/barbouillech/status/1878881144013500489>) gescheitert.

Ein Blick in die VOX-Analyse zu dieser Volksabstimmung

([https://vox.gfsbern.ch/wp-](https://vox.gfsbern.ch/wp-content/uploads/2021/04/d_vox_schlussbericht_def.pdf)

[content/uploads/2021/04/d_vox_schlussbericht_def.pdf](https://vox.gfsbern.ch/wp-content/uploads/2021/04/d_vox_schlussbericht_def.pdf)) reicht,

um zu wissen, dass ganz andere Faktoren eine Rolle spielten. Seit

1977 befragt das Marktforschungsinstitut gfs.bern mit seiner VOX-

Analyse (<https://vox.gfsbern.ch/de/>) nach Volksabstimmungen

Stimmberechtigte, um in Erfahrung zu bringen, aus welchen

Gründen sie für oder gegen eine Gesetzesvorlage abgestimmt

haben.

Die Analyse zur E-ID-Gesetz-Abstimmung von 2021 zeigt, dass bei den Motiven des Nein-Lagers der Datenschutz und die Rolle des Staates hauptsächlich eine Rolle spielten. Die Rolle der privaten Herausgeber der E-ID war untergeordnet.

Die Bedenken drehten sich also generell um den Datenschutz – nicht primär darum, ob private Unternehmen oder der Staat die E-ID herausgeben sollten. Hier wird deutlich, dass der Bundesrat nur nach einem vorgeschobenen Grund suchte, um das E-ID-Gesetz neu aufzugleisen.

Doch selbst die Behauptung, die neue E-ID sei rein staatlich, hält einer Prüfung nicht stand. Das Bundesamt für Polizei (fedpol) ist auf private Partner angewiesen. So vergab

<https://www.eid.admin.ch/de/elca-gewinnt-die-ausschreibung-zur-online-verifikation-der-antragsstellenden-im-e-id-ausstellungsprozess-d>) es die Online-Verifikation der Antragsteller an das Lausanner IT-Unternehmen ELCA Informatique SA. Zudem lässt sich die Bundeswallet-App – die digitale Brieftasche, in der die Identität gespeichert wird – ausschließlich über **Google Play und den Apple App Store** (<https://www.digitale-gesellschaft.ch/event/netzpolitischer-abend-zu-stand-der-entwicklung-der-staatlichen-e-id/>) herunterladen. Schweizer Bürger sind damit total von Big Tech abhängig. Wenn der Bundesrat behauptet, die neue E-ID sei nun „staatlich“, ist das nichts anderes als ein Etikettenschwindel.

Unzureichender Datenschutz

Die E-ID sei angeblich „sicher“, die Sorgen um den Datenschutz unbegründet – so lautet das Mantra des Ja-Lagers. Doch schon ein kurzer Blick auf die Fakten lässt Zweifel aufkommen. Zuständig für Speicherung und Verwaltung der Daten ist das Bundesamt für Polizei. Dass ausgerechnet diese Behörde das Vertrauen der Bürger wecken soll, wirkt fragwürdig. Erst kürzlich geriet das fedpol wegen eines **Hackerangriffs** (<https://www.watson.ch/schweiz/digital/419698936-hackerangriff-daten-von-fedpol-im-darknet-veroeffentlicht>) in die Schlagzeilen: Heikle Daten tauchten daraufhin im Darknet auf.

Auch der Ausstellungsprozess, geregelt in **Art. 17** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_17) des Gesetzes, ist datenschutzrechtlich problematisch. Wer eine E-ID beantragt, muss ein Gesichtsvideo einreichen – das sogenannte Video-Ident-Verfahren. Dabei wird das vorgezeigte Ausweisdokument mit der Person im Videobild abgeglichen und auf Echtheit geprüft. Doch die Technik hat eine Schwachstelle: Deep-

Fake-Videos sind mittlerweile weit verbreitet. Mit im Netz kursierenden Fotos, die praktisch jeder Mensch in sozialen Medien teilt, lassen sich täuschend echte Fälschungen erstellen. Das Risiko: Digitale Identitäten könnten relativ leicht erschlichen werden.



Im Rahmen der Abstimmungskampagne habe ich gemeinsam mit anderen Bürgerrechtsaktivisten im gesamten Kanton Zürich Plakate gegen das E-ID-Gesetz aufgestellt.

Ein warnendes Beispiel liefert Deutschland. Dort gelang es dem Chaos Computer Club, sich über schlecht gesicherte Arztpraxen **Zugang zu tausenden elektronischen Patientenakten zu verschaffen** (<https://www.ccc.de/de/updates/2022/chaos-computer-club-hackt-video-ident>). Warum sollte die Schweiz vor ähnlichen Szenarien gefeit sein? Dass der Bund selbst die Gefahr nicht ausschließt, zeigt ein Blick ins Gesetz. Gemäß **Art. 27** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_27) werden die Daten zwanzig Jahre lang gespeichert, biometrische Daten erst fünf Jahre nach Ablauf der E-ID gelöscht. Diese lange Frist lässt nur einen Schluss zu: Der Bund rechnet mit Identitätsdiebstahl und will im Ernstfall Rückverfolgungen ermöglichen. Indirekt gibt er damit zu, dass jemand jahrelang unter falscher Identität eine E-ID nutzen könnte.

Trügerische Freiwilligkeit

Die Befürworter betonen stets die Freiwilligkeit der E-ID. Doch ein genauer Blick ins Gesetz zeigt: Von echter Freiwilligkeit kann keine Rede sein. **Art. 24** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_24) verpflichtet alle Behörden und Stellen mit öffentlichen Aufgaben, die E-ID zu akzeptieren. **Art. 25** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_24) sieht zwar vor, dass auch ein Pass nach **Art. 14** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_24) akzeptiert werden muss – doch nur, wenn die Person „persönlich erscheint“. Das klingt nach einer Wahlmöglichkeit, ist in der Praxis aber eine Mogelpackung. Bei Online-Diensten wie Instagram, Netflix oder im E-Commerce kann niemand „persönlich erscheinen“. Damit bleibt faktisch nur die E-ID. Die Folge: Für fast alle digitalen Aktivitäten wird die E-ID zwingend.

Beispiele aus Österreich, Schweden oder **Estland**

(<https://www.nzz.ch/international/e-id-in-estland-ohne-digitale-identitaet-bist-du-niemand-ld.1755983>) zeigen, wie schnell eine digitale Identität vom angeblich freiwilligen Angebot zum faktischen Zwang wird. Wer sie nicht nutzt, kann grundlegende Dinge des Alltags kaum noch erledigen.

Auch in der Schweiz wird die E-ID zur Voraussetzung für zentrale Dienste. Einen Strafregisterauszug per Brief zu bestellen, wird nicht mehr möglich sein – nur noch mit E-ID oder durch persönliches Erscheinen am Schalter. Das Organspenderegister soll künftig ausschließlich über die E-ID zugänglich sein, ebenso das elektronische Patientendossier, das so zum Standard gemacht wird.

All das sind Formen eines indirekten Zwangs, der die behauptete Freiwilligkeit untergräbt. Hinzu kommt: **Art. 31** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_31) erlaubt den Kantonen, zusätzliche Gebühren zu erheben, wenn Bürger Dienstleistungen vor Ort statt digital mit der E-ID beziehen. Wer keine E-ID will, muss also draufzahlen. Was als „freiwillig“ verkauft wird, bedeutet in Wahrheit Abhängigkeit – und eine schleichende Diskriminierung all jener, die ihre Identität nicht dem elektronischen Zugriff ausliefern wollen.

Ausgehebelte Volksrechte

Mit dem E-ID-Gesetz droht ein weiterer Abbau der Volksrechte. **Art. 30**

(https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_31) gibt dem Bundesrat weitreichende Befugnisse: Er darf die Vertrauensinfrastruktur und das Informationssystem der E-ID eigenmächtig um zusätzliche Elemente erweitern – auch um besonders schützenswerte Personendaten wie

Gesundheitsinformationen oder Angaben zur politischen Betätigung. Erst nach bis zu zwei Jahren muss er das Parlament um Genehmigung bitten. Bleibt diese aus, fällt die Regelung zwar weg – doch in dieser Zeit könnte der Bundesrat längst Fakten geschaffen haben. Mit anderen Worten: Zwei Jahre lang könnte er per Verordnung neue, sensible Datenfelder in die E-ID aufnehmen, ohne dass Volk oder Parlament einbezogen würden. Die Erfahrung zeigt, dass der Bundesrat solche Spielräume regelmäßig nutzt, um Vorschriften einzuführen. Ein naheliegendes Beispiel wäre ein digitaler Gesundheitspass über die E-ID, der in einer Krise flächendeckend verlangt würde. Das ist eine massive Kompetenzdelegation, die Volksrechte unterläuft.

Noch weiter geht **Art. 32**

(https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_32): Er ermächtigt den Bundesrat, „völkerrechtliche Verträge selbstständig abzuschließen“. Das bedeutet, er könnte internationale Abkommen zur E-ID ohne jede Mitsprache von Volk und Parlament unterzeichnen. Offiziell soll dies die Nutzung und rechtliche Anerkennung der Schweizer E-ID im Ausland erleichtern – sowie die Anerkennung ausländischer E-IDs in der Schweiz. Doch die Vorlage räumt dem Bundesrat zusätzlich das Recht ein, sämtliche Bestimmungen zur Umsetzung solcher Verträge eigenmächtig zu erlassen. Spätestens wenn die EU ihr eigenes E-ID-System vollständig etabliert, könnte der Bundesrat die Vorgaben aus Brüssel direkt in die Schweiz übernehmen – ohne dass die Stimmbürger jemals darüber entscheiden dürfen.

Fehlende Transparenz

Bundesrat und Befürworter beteuern, die E-ID sei transparent. Das stimmt jedoch nicht. Echte Transparenz würde voraussetzen, dass der Quellcode der Software offengelegt wird. Doch genau das

schließt das E-ID-Gesetz aus: Gemäß **Art. 12** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_12) darf der Quellcode aus Gründen des Drittrechtsschutzes oder der Sicherheit geheim bleiben. Von Open Source kann also keine Rede sein. Art. 12 Abs. 1 verpflichtet das Bundesamt für Informatik und Telekommunikation (BIT) zwar, den Quellcode der Vertrauensinfrastruktur offenzulegen. Auf den ersten Blick klingt das nach Transparenz. Doch Abs. 2 schränkt diese Pflicht massiv ein: Der Quellcode oder Teile davon werden nicht veröffentlicht, wenn „Rechte Dritter oder sicherheitsrelevante Gründe dies ausschließen oder einschränken würden“. Im ursprünglichen Entwurf war nur von sicherheitsrelevanten Gründen die Rede – das Parlament fügte die Klausel zu den „Rechten Dritter“ hinzu. Damit haben private Anbieter, die dem Bund Software liefern, ein einfaches Einfallstor: Unter Berufung auf Lizenzrechte kann die Einsicht verweigert werden.

Die Öffentlichkeit erfährt dann nicht, welche Programme im Hintergrund laufen und wie die Daten verarbeitet werden. Eine echte Kontrolle wird so verunmöglicht. Wer ein System mit so sensiblen Daten aufbaut, müsste im Gegenteil sicherstellen, dass die Öffentlichkeit genau nachvollziehen kann, wie die Technik funktioniert.

Der Bund setzt stattdessen auf **Security by Obscurity** (https://de.wikipedia.org/wiki/Security_through_obscurity) – also den Versuch, Sicherheit durch Geheimhaltung der Funktionsweise zu erreichen. Fachleute kritisieren diesen Ansatz seit Jahren. Das US-amerikanische National Institute for Standards and Technology **rät ausdrücklich davon ab** (https://en.wikipedia.org/wiki/Security_through_obscurity).

Umfassende Überwachung

Mit der E-ID erhält der Staat ein Instrument, seine Bürger auf Schritt und Tritt zu überwachen. Physische Ausweise hinterlassen kaum digitale Spuren: Sie werden selten verlangt und die Daten in der Regel nicht gespeichert. Bei der E-ID ist es anders. Jedes Vorweisen des elektronischen Nachweises erzeugt personenbezogene Daten, die gespeichert werden. Damit eröffnet sich dem Staat ein Überwachungsinstrument, das die Kontrollmöglichkeiten totalitärer Systeme des 20. Jahrhunderts bei Weitem übertrifft – und eine erhebliche Gefahr für die Grundrechte in der Schweiz darstellt.

Die Befürworter versprechen, es würden keine Nutzerprofile erstellt und alles bleibe anonym. Doch schon **Art. 10 Abs. 3** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_10) zeigt die Schwachstelle: Das BIT erhalte zwar keine Einsicht in die Inhalte der Nachweise – außer aufgrund der durch die Abfragen generierten Daten. Mit jeder Abfrage, mit jedem Login fallen beim BIT Metadaten an: IP-Adressen, Zeitstempel, Portnummern und mehr. Damit entsteht ein umfassendes Datenpaket, das zentral gespeichert wird. **Die Art. 2 und 3** (https://www.fedlex.admin.ch/eli/fga/2025/20/de#art_2) des Gesetzes regeln die Register beim BIT. Auch dort heißt es, eine direkte Zuordnung zu Personen sei nicht vorgesehen. Doch wieder gibt es Ausnahmen: Personendaten, die beim Abfragen des Basisregisters anfallen, dürfen sehr wohl namentlich ausgewertet werden – erlaubt durch **Art. 57o Abs. 1 lit. a und b des Regierungs- und Verwaltungsorganisationsgesetz (RVOG)** (https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/de#art_57_o), etwa bei „konkretem Verdacht auf Missbrauch“ oder zur „Abwehr konkreter Bedrohungen“.

Ein bloßer Verdacht genügt also, um Login-Daten zu durchleuchten. Über IP-Adressen und Timestamps lassen sich Geräte, Betriebssysteme und Nutzungsgewohnheiten identifizieren. Der Staat könnte

daraus ein detailliertes Profil erstellen: wann, wie oft und zu welchen Zeiten sich eine Person einloggt.

Hinzu kommen mögliche Provider-Abfragen, die sogar besuchte Domains oder Geodaten von Mobilfunkmasten preisgeben. So bleibt nur eine hauchdünne Grenze zwischen angeblich anonymer Nutzung und faktischer Nachverfolgbarkeit. Schon bei geringstem Verdacht kann die Identität offengelegt werden. Die Möglichkeit zum Machtmissbrauch ist damit im Gesetz angelegt – und jede Erfahrung zeigt: Was der Staat an Befugnissen erhält, nutzt er auch.

There is no such thing as a free lunch

Ein weiterer Mythos des Ja-Lagers lautet, die staatliche E-ID sei kostenlos. Doch staatliche Leistungen werden stets vom Steuerzahler finanziert – und können daher niemals wirklich gratis sein. Ungeachtet dessen ist das Schweizer E-ID-Projekt alles andere als billig: Zwischen 2023 und 2028 sind rund **180 Millionen Franken** (https://www.admin.ch/dam/gov/de/Dokumentation/Abstimmungen/September2025/Bar_Erlaeuterungen_September_2025_de_v2.pdf.download.pdf/Bar_Erlaeuterungen_September_2025_de_v2.pdf) für Entwicklung und Betrieb der Infrastruktur vorgesehen. Ab 2029 kommen jährlich etwa **25 Millionen Franken** (<https://notebooklm.google.com/notebook/9c5419fc-e1fc-40d4-85fd-eeee0e6c89b4>) an laufenden Kosten hinzu. Diese horrenden Summen tragen letztlich alle Steuerzahler – auch jene, die die E-ID gar nicht nutzen wollen.

Es braucht keine E-ID

Es stellt sich die Frage: Wozu braucht es überhaupt einen digitalen Identitätsnachweis? Der Bund nennt zwei Gründe. Erstens soll die

E-ID für **Behördengänge**

(<https://www.fedlex.admin.ch/eli/fga/2023/2842/de>) erforderlich sein. Doch dafür existiert bereits ein **offizielles Behörden-Login** (<https://www.agov.admin.ch/de>) – eine zusätzliche E-ID ist überflüssig. Zweitens soll sie der Altersverifikation im Alltag dienen, etwa im Supermarkt oder am Kiosk. Doch auch hier reicht die physische Identitätskarte völlig aus. Sie ist sogar die bessere Lösung, weil sie keine digitalen Spuren hinterlässt und die Daten wirksamer schützt. Kurzum: Die herkömmlichen Ausweise sind der E-ID sowohl in Bezug auf Sicherheit als auch auf Datensparsamkeit klar überlegen.

Referendumskampagne im Endspurt

Die Abstimmungskampagne befindet sich in der Schlussphase. In aller Ausführlichkeit habe ich darzulegen versucht, warum das Schweizer E-ID-Gesetz gefährlich, unnötig und daher abzulehnen ist. Ich hätte noch weitere Punkte aufzählen und noch mehr ins Detail gehen können, doch dies hätte den Rahmen gesprengt. Die Bürgerrechtsbewegung MASS-VOLL!, der ich selbst angehöre, hat im Januar das Referendum ergriffen und mit ihren gesammelten Unterschriften entscheidend dazu beigetragen, dass das Schweizer Volk am 28. September über diese Gesetzesvorlage abstimmen kann. Falls Sie, geschätzter Leser, Schweizer Staatsbürger sind und die drohende digitale Identität an der Urne versenken wollen: Unterstützen Sie bitte jetzt die Referendumskampagne von MASS-VOLL!. Weitere Informationen finden Sie **hier** (<https://e-id.massvoll.swiss/>).



Unterstützen (<https://e-id.massvoll.swiss/>) Sie jetzt die Referendumskampagne gegen das E-ID-Gesetz!

Die Schweiz steht an einem Scheideweg: Entweder sie wehrt die totalitären Pläne des Bundesrates ab – oder sie macht einen gewaltigen Schritt in Richtung totaler Überwachungsstaat.

Verglichen mit der Einführung der E-ID wirkt selbst die **Fichenaffäre**

(<https://de.wikipedia.org/wiki/Fichenskandal>) wie ein Kindergeburtstag. Damals, 1989, wurde durch eine parlamentarische Untersuchung aufgedeckt, dass die Bundespolizei über Jahrzehnte hinweg fast eine Million Menschen systematisch überwacht hatte – ein Skandal, der das Vertrauen in den Staat erschütterte. Heute aber haben die Schweizer als einziges Volk der Welt das Privileg, über die E-ID an der Urne selbst zu entscheiden und der aggressiven Überwachungsoffensive des Staates einen Riegel vorzuschieben.

Redaktionelle Anmerkung: Dieser Beitrag erschien zuerst unter dem Titel „**Der digitale Fichenstaat**“ (<https://www.straumedien.ch/p/der-digitale-fichenstaat>)“ bei

[StrauMedia](<https://www.straumedia.ch>) und dem Portal der **Freien Akademie für Medien und Journalismus** (<https://www.freie-medienakademie.de/medien-plus/der-digitale-fichenstaat>).



Michael Straumann, Jahrgang 1998, studiert Politikwissenschaft und Philosophie an der Universität Zürich und arbeitet als redaktioneller Praktikant für die Zeitschrift **Schweizer Monat**. Zudem engagiert er sich bürgerrechtlich. Zwei Jahre lang war er als Vorstandsmitglied der Schweizer Bürgerrechtsbewegung **MASS-VOLL!** tätig. An mehreren Referenden hat er aktiv mitgewirkt, darunter im Leitungsteam des dritten Referendums gegen das Covid-Gesetz. Aktuell sitzt er im Komitee der Souveränitätsinitiative, die grundrechtswidrige internationale Verträge wie den WHO-Pandemiepakt in der Schweiz verhindern möchte. Weitere Informationen auf **StrauMedia** (<https://www.straumedia.ch/>).