Samstag, 09. August 2025, 15:58 Uhr
~11 Minuten Lesezeit

Gefährliche Sicherheit

Mit Scheinargumenten greift der politisch-digitale Machtapparat die Freiheit des Internets an und bastelt an der Vervollkommnung des Überwachungsstaats.

von Tom-Oliver Regenauer
Foto: Trismegist san/Shutterstock.com

Digitale Identifikationssysteme sollen Online-Zugänge und Ausweise sicherer machen und Minderjährige vor sensiblen Inhalten schützen. Doch wie aktuelle Entwicklungen in Großbritannien, Australien und der

EU verdeutlichen, markieren solche Systeme vor allem das Ende des freien Internets. Das sollte speziell Schweizer Stimmbürger alarmieren. Denn sie haben das einzigartige Privileg, am 28. September 2025 selbst über die Einführung der E-ID entscheiden zu dürfen.

Es passiert überall und gleichzeitig: in Deutschland (https://www.cdu.de/app/uploads/2025/04/KoaV-2025-Gesamt-final-0424.pdf), Österreich (https://www.id-austria.gv.at/de/verwenden/app-id-austria), Frankreich (https://www.service-public.fr/particuliers/actualites/A18208?lang=en), Portugal (https://www.gov.pt/servicos/adicionar-documentos-de-identificacao-na-app-id-gov-pt), Italien (https://www.cartaidentita.interno.gov.it/en/cie/electronic-identity-card/), und um es abzukürzen: Es passiert europaweit (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de). Aber auch die USA (https://www.tsa.gov/real-id), Russland (https://www.biometricupdate.com/202506/russia-launching-digital-id-super-app-inspired-by-chinese-wechat), die Ukraine (https://expo.diia.gov.ua/), Australien (https://www.digitalidsystem.gov.au/what-is-digital-id) und Großbritannien (https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer) machen mit. Überall ist, oder wird, eine digitale Identität implementiert. Die sogenannte E-ID.

> ***Die gängige Begründung für den konzertierten Rollout des elektronischen Identitätsnachweises ist, dass man Minderjährige damit vor schädlichen Online-Inhalten schützen und die „Verbreitung von Desinformation“***

> ***eindämmen wolle.***

Fügt man diesen beiden staatlich ventilierten Argumenten noch hinzu, dass es mit der E-ID bequemer wird, sich auszuweisen, weil man das Smartphone mit dem betreffenden Wallet ohnehin immer dabei habe, hat man auch schon alle drei Begründungen zusammen, die sich für so eine E-ID finden lassen. Mehr gibt es nämlich nicht — und fadenscheinig sind sie obendrein.

Risiken gibt es dagegen en masse, wie die aktuellen Entwicklungen in Großbritannien und Australien belegen. Bereits im Februar 2025 kündigte beispielsweise **Apple** (https://support.apple.com/en-us/122234) an, seine Advanced Data Protection (Verschlüsselung) im Vereinten Königreich aufgrund des „**Online Safety Act** (https://www.wired.com/story/the-uks-controversial-online-safety-act-is-now-law/)“ einstellen zu müssen, und tat dies auch. Denn die britische Regierung wies das Unternehmen an, eine Hintertür für den Zugriff auf verschlüsselte iCloud-Daten einzurichten. Apple wehrt sich und **klagt** (https://reclaimthenet.org/uk-tribunal-rejects-secret-case-apple-encryption-press-freedom). Unterstützt wird der Konzern dabei von **WhatsApp** (https://www.bbc.com/news/articles/cgmjrn42wdwo), wo man sich der gleichen Forderung ausgesetzt sieht. Eine Entscheidung steht aus. Kurze Zeit später, im Mai 2025, passte **Bitchute** (https://www.bitchute.com/ukregulation) seine Plattform für britische Nutzer so an, dass in Großbritannien hochgeladene Inhalte für britische Nutzer nicht mehr angezeigt werden. Nur so konnte das Unternehmen sicherstellen, weiterhin auf der Insel verfügbar zu sein, ohne den überwachungsstaatlichen Forderungen der britischen Behörden Folge leisten zu müssen.

Aber das war nur der Anfang. Seit Freitag, 25. Juli 2025, überschlagen sich die **Ereignisse** (https://arstechnica.com/tech-policy/2025/07/vpn-use-soars-in-uk-after-age-verification-laws-

go-into-effect/) auf der Insel förmlich. Denn erst zu diesem Termin entfaltete das neue Gesetz sein volles „Potenzial“. Meint: Wer seitdem in Großbritannien auf Pornografie zugreifen will, muss sich ausweisen. Die zuständige Medienaufsichtsbehörde **Ofcom** (https://en.wikipedia.org/wiki/Ofcom) teilte diesbezüglich mit, dass schon jetzt über 6.000 Webseiten eine entsprechende Altersverifikation durchführen. Dass es dabei nicht um den Schutz Minderjähriger vor pornografischen Inhalte geht, bewiesen in den vergangenen Tagen unter anderem Reddit, Bluesky, Spotify oder **Microsofts Xbox** (https://www.theverge.com/news/714458/microsoft-xbox-age-verification-uk-social-features), denn auch dort werden für „soziale Angebote“ nun biometrische Altersnachweise gefordert. Selbst **Pizza Hut** (https://x.com/Pirat_Nation/status/1951019582073753612) scheint jetzt einen Ausweis sehen zu wollen. Und Spotify **droht** (https://reclaimthenet.org/spotify-threatens-to-delete-accounts-that-fail-digital-id-checks) Nutzern gar damit, das Konto zu löschen, sollten diese den Verifikationsanforderungen nicht zeitnah Folge leisten.

Kaum verwunderlich also, dass der Zugriff auf VPN-Dienstleister auf der Insel am letzten Wochenende sprunghaft anwuchs. So vermeldete zum Beispiel **Proton VPN** (https://x.com/ProtonVPN/status/1948773319148245334), dass die Bestellungen von Kunden aus Großbritannien praktisch über Nacht um 1.400 Prozent angestiegen waren. Wer nicht schnell genug handelte, hatte das Nachsehen. Denn mittlerweile haben Internetdienstleister (ISPs) wie Virgin Media den Zugriff auf die Webseiten von VPN-Anbietern wie Proton, Nord, Express oder Mullvad **blockiert** (https://x.com/gnukeith/status/1950395286221651999) — man kann deren Software also gar nicht mehr herunterladen. Außer man weiß sich anders zu helfen. Zum Beispiel durch manuelle Eingabe von DNS-Adressen auf dem heimischen Router. Illegale Streaming-

Seiten funktionieren in Großbritannien übrigens auch nicht mehr. Genau wie **TOR** (https://x.com/gnukeith/status/1950670553674916106).

Denn parallel zum Rollout des digitalen Altersnachweises hat der amerikanische DNS-Dienstleister **Cloudflare** (https://de.wikipedia.org/wiki/Cloudflare) den VPN-Zugriff auf über 200 Streaming-Domains blockiert. Fürs Erste. Und Google **verweigert** (https://www.computerworld.com/article/4031422/google-wont-say-whether-the-uk-govt-is-breaking-its-encryption.html) die Auskunft darüber, ob die britische Regierung bereits Zugang zu verschlüsselten Daten der hauseigenen Dienste hat oder nicht.

In Australien sieht es kaum besser aus, weshalb Signal-Chefin **Meredith Whittaker** (https://www.msn.com/en-au/money/markets/signal-warns-it-will-leave-australia-if-forced-to-hand-over-messages/ar-AA1JCtWu) am 31. Juli 2025 ankündigte, den australischen Markt zu verlassen, wenn die Regierung weiterhin darauf bestehe, dass der Messengerdienst Kundendaten herausgibt oder seine Verschlüsselung kompromittiert. Auch **Suchmaschinen** (https://x.com/senatorbabet/status/1950758760538157451) wie Google und Bing werden in „Down Under" bald nur noch mit Identitätsnachweis funktionieren. VPN-Anbieter dürften nach **Angaben** (https://x.com/senatorbabet/status/1950760728505577721) des Senators für den Distrikt Victoria ebenfalls dazu gezwungen werden, ihre Nutzer zu identifizieren.

Das Empire lässt grüßen. Pikantes Detail: Ein Großteil der in Australien angefragten Altersverifikationen läuft über das **israelische** (https://en.wikipedia.org/wiki/AU10TIX) Unternehmen **AU10TIX** (https://www.au10tix.com/), dessen Gründer, Ron Atzmon, seinen Militärdienst bei der berüchtigten **Schin-Bet** (https://de.wikipedia.org/wiki/Schin_Bet)-Spezialeinheit **Unit**

8200 (https://de.wikipedia.org/wiki/Unit_8200) ableistete. AU10TIX erstellt „digitale Zwillinge“ seiner Kunden. Sprich: Avatare, die alle Daten zusammenziehen, die ihre organischen Kopiervorlagen je erzeugt haben. ***L'Orient-Le Jour*** *(https://today.lorientlejour.com/article/1351162/how-israeli-tech-is-leaving-lebanon-by-the-wayside.html)* schrieb diesbezüglich am 2. Oktober 2023:

„Ron Atzmon, der Gründer von AU10TIX, diente während seines Militärdienstes bei der berüchtigten Unit 8200 des Schin Bet. Mit 5.000 bis 10.000 Mitarbeitern ist diese Gruppe Israels wichtigste Geheimdiensteinheit und liefert dem Land 90 Prozent seines Geheimdienstmaterials, wie Yair Cohen, der die Einheit fünf Jahre lang leitete, gegenüber Forbes erklärte. Die Einheit stand 2010 medial im Fokus, als Stuxnet entdeckt wurde, ein bösartiger Computerwurm, der gemeinsam mit der CIA entwickelt wurde, um Teherans Nuklearausrüstung umzuprogrammieren und unschädlich zu machen. Der Erfolg der Operation warf die Entwicklung des iranischen Atomprogramms um mehrere Jahre zurück. Unit 8200 ist mehr als nur eine Militäreinheit. Sie dient als Inkubator für Israels Technologieindustrie, die 14 Prozent der Arbeitsplätze des Landes und fast 20 Prozent seines BIP ausmacht. Waze, Wix, Viber und NSO, die die berüchtigte Spyware Pegasus produzierten, haben eines gemeinsam: Ihre Gründer sind ehemalige Mitglieder der Unit 8200.“

AU10TIX ist übrigens auch für die biometrische Identifikation von Nutzern bei **Twitter** (https://www.mintpressnews.com/identity-verification-or-data-exposure-twitter-using-israeli-tech-firm-headed-by-ex-military-officials-to-verify-users/286156/) oder für die **Verified ID** (https://learn.microsoft.com/de-de/entra/verified-id/howto-verifiable-credentials-partner-au10tix) von Microsoft verantwortlich. Unter anderem. Zieht man nun in Betracht, dass alle Big-Tech-**Entwicklungen** (https://www.businessinsider.com/the-us-military-is-responsible-for-almost-all-the-technology-in-your-iphone-2014-

10) und -Konzerne von **DARPA** (https://thebreakthrough.org/issues/energy/the-iphone-and-the-invisible-hand-of-government), **In-Q-Tel** (https://en.wikipedia.org/wiki/In-Q-Tel) (CIA) und US-Militär startfinanziert wurden — siehe zum Beispiel den Artikel „How the CIA made Google“ vom 22. Januar 2015 — oder dass Elon Musks xAI jüngst Twitter **gekauft** (https://x.com/elonmusk/status/1905731750275510312) hat und Microsoft, xAI, BlackRock, MGX und Nvidia im März 2025 ein **Konsortium** (https://www.reuters.com/technology/artificial-intelligence/nvidia-xai-join-microsoft-blackrock-develop-ai-infrastructure-2025-03-19/) zur Weiterentwicklung von künstlicher Intelligenz (KI) gegründet haben, ein Bereich, den Peter Thiels Spionagekonzern Palantir zusammen mit Accenture Federal Services **leitet** (https://newsroom.accenture.com/news/2025/palantir-and-accenture-federal-services-join-forces-to-help-federal-government-agencies-reinvent-operations-with-ai), bekommt man eine Vorstellung davon, welche Strukturen von E-ID, „Big Data“ und Biometrie profitieren. Der Bürger ist es jedenfalls nicht.

So verwundert es kaum noch, dass der neue Federal Chief Information Officer (FCIO) der Vereinigten Staaten, **Gregory Barbaccia** (https://www.piratewires.com/p/palantirs-former-head-of-intelligence-has-a-new-quest?f=home), zuvor bei Palantir für „interne Sicherheit“ und „Investigationen“ verantwortlich zeichnete. Bei einem Unternehmen, dessen initialen Algorithmus — „Igor“ — Peter Thiel schon im Jahr 2000 für seine damalige Firma **PayPal** (https://nymag.com/intelligencer/2020/09/inside-palantir-technologies-peter-thiel-alex-karp.html) entwickelte und dessen einziger Kunde in den ersten acht Jahren die CIA war.

Vielleicht beginnt **YouTube** (https://support.google.com/youtube/thread/356191968/extending-protections-to-more-us-based-teens?hl=en) ja deshalb am 13.

August 2025, das Alter seiner amerikanischen Nutzer mit KI zu überwachen, obwohl Gesetze wie der britische Online Safety Act in den USA noch gar nicht gelten. Ersatzweise gab **Donald Trump** (https://x.com/disclosetv/status/1950663423018082342) am 30. Juli 2025 aber bekannt, dass die USA ein „Digital Health Tech Ecosystem" lancieren werden, um das „Gesundheitswesen ins digitale Zeitalter zu führen". Dafür vertraue man auf die Dienste von Apple, Microsoft, Google, Amazon, OpenAI und – natürlich – **Palantir** (https://www.usaspending.gov/recipient/1ea8a9a4-3726-3491-9040-66950bb67606-P/latest). Schließlich hat Peter Thiels Spionagekonzern gerade erst einen **10-Milliarden-Deal** (https://www.cnbc.com/2025/08/01/palantir-lands-10-billion-army-software-and-data-contract.html) mit dem Verteidigungsministerium unterschrieben, den bislang größten in der US-Geschichte. Darüber hinaus steht in den USA die Verabschiedung des **Block BEARD Act** (https://www.tillis.senate.gov/services/files/24A0311C-E658-4440-A259-AA8A876115E6) bevor, eines Gesetzes, das der US-Regierung erstmals erlaubt, **Webseiten** (https://copyrightalliance.org/press-releases/statement-on-block-beard-act/) zu sperren. **Reclaim The Net** (https://reclaimthenet.org/us-lawmakers-block-beard-bill-website-censorship-piracy) nennt es einen »potentzellen Internet Kill Switch«.

Für die EU gilt laut **Android Headlines** (https://www.androidheadlines.com/2025/07/eu-age-verification-app-to-ban-android-apps-not-licensed-by-google.html) unterdes der Plan, „die Altersverifizierungs-App um eine Integritätsprüfung für Android-Apps zu erweitern. Dies würde den Nutzer verpflichten, nur lizenzierte und installierte Apps aus dem Google Play Store zu verwenden. Die Authentizität der App wird mithilfe des Google Play Integrity-Dienstes ermittelt und verifiziert". Wer also mit alternativen Betriebssystemen arbeitet oder einen VPN auf dem Smartphone nutzt, wird die EUDI

(European Digital Identity) vermutlich nicht nutzen können. Die nur noch auf deren Vorlage hin zugänglichen sozioökonomischen Strukturen aber auch nicht.

Am 29. Juli 2025 vermeldete **Tech Radar** (https://www.techradar.com/computing/cyber-security/after-the-uk-online-age-verification-is-landing-in-the-eu), dass fünf EU-Mitgliedsstaaten, namentlich Dänemark, Spanien, Frankreich, Italien und Griechenland, in Kürze den Prototyp einer **EU-Applikation** (https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1820) zur Altersverifikation testen werden. Die „Wiege der Demokratie" hat bereits im Januar 2025 **angekündigt** (https://www.telepolis.de/features/Totale-Kontrolle-Griechenland-verknuepft-Steuer-ID-mit-Social-Media-10222907.html), die Profildaten von Steuerpflichtigen mit deren Social-Media-Konten zu verknüpfen, um Kinder und Jugendliche vor sozialen Medien zu schützen. Und Belgien ist gerade im Begriff, Online-Bibliotheken wie das Internet Archive zu sperren, wie eine aktuelle **Verordnung** (https://torrentfreak.com/belgium-targets-internet-archives-open-library-in-sweeping-site-blocking-order/) zeigt.

> ***Das freie Internet steht also auch in der EU vor dem Aus. Wer bislang davon ausging, die EU stehe für Demokratie und Meinungsfreiheit, hat sich offenbar zu wenig mit deren Organisationsstruktur beschäftigt.***

Exemplarisch für diese steht das **INTCEN** (https://de.wikipedia.org/wiki/INTCEN) (EU Intelligence Analysis Center), ein 2003 in Zusammenarbeit mit der CIA gegründetes, inoffizielles Organ der EU, das im Gegensatz zu anderen Nachrichtendiensten nicht dem EU-Parlament untersteht, welches somit weder konsultiert wird noch Einsichtsrechte hat. Gleiches gilt für nationale Parlamente, weil das INTCEN als inoffizielles Organ gewertet wird. Die im Verborgenen agierende Behörde **kollaboriert**

(https://euintelligence.com/intelligence/european-union-intelligence-and-situation-centre-eu-intcen/) mit dem European Strategic Intelligence and Security Center (ESISC) und ist zuständig für die Vernetzung von Nicht-EU-Staaten und EU mittels des **Berner Clubs** (https://de.wikipedia.org/wiki/Berner_Club), einem intransparenten, informellen Zusammenschluss von Direktoren der Inlandsgeheimdienste der 27 EU-Mitgliedstaaten sowie Norwegens und der Schweiz.

> ***Je mehr solcher Mosaiksteine man zusammenfügt, desto deutlicher wird, was digital-finanzieller Komplex, Geheimdienste und supranationale Institutionen wie die EU und die Vereinten Nationen (UN) da unter weitgehendem Ausschluss der Öffentlichkeit aufgleisen: den Überwachungs- und Polizeistaat des digitalen Zeitalters.***

Dass der Rollout der ID-Ökosysteme nahezu weltweit parallel vonstatten geht und sowohl **Russland** (https://www.biometricupdate.com/202506/russia-launching-digital-id-super-app-inspired-by-chinese-wechat) als auch **Elon Musk** (https://www.theguardian.com/media/2023/jul/29/elon-musk-wechat-twitter-rebranding-everything-app-for-west) dabei von der chinesischen WeChat-App inspiriert sind, ist kein Zufall. Dass die österreichische Regierung schon jetzt **ankündigt** (https://www.id-austria.gv.at/de/verwenden/app-id-austria), dass die „ID Austria"-Applikation „einen einfachen Weg zu Services der Verwaltung und privater Unternehmen" darstellen wird, ebenfalls nicht. Denn es braucht wenig Fantasie, um zu prognostizieren, dass neben der elektronischen Patientenakte, dem digitalen Führerschein, der Sozialversicherungsnummer und den biometrischen Daten auch die Steuern, Krankenkassendaten, digitalen Währungen und Social-Media-Konten über das Bürger-Wallet verknüpft werden sollen. Nicht umsonst **spricht** (https://web.archive.org/web/20211013100817/https:/dserver.bundestag.de/btd/19/319/1931992.pdf) das deutsche

Bundesministerium für Bildung und Forschung (BMBF) seit Jahren von der Einführung eines „Bonus Systems“: von einen Sozialpunkte- oder Sozialkreditsystem nach chinesischem Vorbild.

Der globale Rollout digitaler Identifikationssysteme basiert auf **Nachhaltigkeitsziel 16.9** (https://sustainabledevelopment.un.org/topics/sustainabledevelopmentgoals) der Agenda 2030 der Vereinten Nationen, deren Erfüllung sich alle 193 UN-Mitgliedsstaaten verschrieben haben. Operativ heruntergebrochen wird solch ein strategisches Ziel unter anderem vom Weltwirtschaftsforum (WEF) in Davos, das im Juni 2024 zusammen mit der britischen Medienaufsichtsbehörde Ofcom ein **Dokument** (https://dtspartnership.org/press-releases/dtsp-co-chairs-world-economic-forum-white-paper-how-to-measure-digital-safety-effectively-to-reduce-risks-online/) veröffentlichte, dass sich mit der Frage auseinandersetzt, „wie digitale Sicherheit effektiv gemessen werden kann, um Online-Risiken zu reduzieren“. Weitergeführt werden die darin beschriebenen Gedanken in einem **WEF-Report** (https://reports.weforum.org/docs/WEF_The_Intervention_Journey_A_Roadmap_to_Effective_Digital_Safety_Measures_2025.pdf) vom März 2025, der den Titel „Die Interventionsreise: Eine Wegleitung für effektive digitale Sicherheitsmaßnahmen“ trägt. Synopsis: Nur die digitale Identität und ein lückenlos kontrolliertes Internet können das Überleben der Spezies Mensch sicherstellen.

Neben Prozessdesign, technischen Konzepten und Rollout-Planungen steht bei solchen Dokumenten aber vor allem das Marketing im Vordergrund — die Frage also, mit welchen Argumenten, Begrifflichkeiten und PR-Maßnahmen man der Öffentlichkeit solch ein kontroverses Projekt schmackhaft machen kann.

Das zeigt sich dieser Tage auch in der Schweiz, dem einzigen Land der Welt, in dem die Bevölkerung das Recht hat, selbst über die

Annahme des hiesigen **E-ID-Gesetzes** (https://www.fedlex.admin.ch/eli/fga/2025/20/de) zu entscheiden, zum zweiten Mal. Denn schon am 7. März 2021 erteilte die Stimmbevölkerung der Einführung einer E-ID eine klare Abfuhr. **64,4 Prozent** (https://www.inside-it.ch/post/nach-der-e-id-pleite-wie-weiter-20210308) lehnten die Vorlage damals ab. Ein deutliches Votum. Das zweite Referendum, das mit **55.344** (https://www.eid.admin.ch/de/e-id-referendum-zustande-gekommen) eingereichten Unterschriften zustande kam, findet am 28. September 2025 statt.

Sollte die Gesetzesvorlage dieses Mal angenommen werden, könnte die entsprechende ID-App namens „Swiju" — für die Namensgebung **zahlte** (https://www.20min.ch/story/namensfindungsprozess-swiyu-fuer-diesen-namen-blaetterte-der-bund-62-300-franken-hin-103388065) der Bund übrigens 62.300 Franken an zwei Texter und einen Markenentwickler aus Köln — ab **Anfang 2026** (https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id.html) ausgerollt werden. Die Entwicklungskosten für die Applikation **belaufen** (https://www.20min.ch/story/trotz-kritik-elektronische-id-auf-der-zielgeraden-das-musst-du-wissen-103227530) sich auf 200 Millionen Franken, der jährliche Betrieb soll künftig 25 Millionen Franken kosten.

Während sich auch für die eidgenössische Variante der digitalen Identität nicht mehr als die drei eingangs erwähnten Pro-Argumente finden lassen und die öffentliche Verwaltung hier besser funktioniert als in jedem anderen Land, birgt die Einführung eines solchen Systems die gleichen Risiken, wie sie nun in Großbritannien, Australien und der EU zutage treten, auch wenn gemäß der neuen Gesetzesvorlage anstelle von privaten Anbietern nun der Staat für den Betrieb zuständig sein soll.

> ***Es drohen Datenklau, Hackerangriffe, Missbrauch durch Dritte, Abhängigkeit von Tech-Konzernen, weil so ein***

> ***System nicht gänzlich ohne Silicon Valley betrieben werden kann, administrative Intransparenz, da der Quellcode nicht veröffentlicht wird, digitale Überwachung, der Verlust von Privatsphäre und Grundrechten sowie die Einschränkung von Presse- und Meinungsfreiheit, während durch das System keinerlei quantifizierbarer Mehrwert generiert wird.***

Denn sichere Identifikationssysteme gibt es durch das Ausweiswesen oder die Zwei-Faktor-Authentifizierung längst. So ist auch nachvollziehbar, wenn das Magazin *Republik* am 7. Mai 2025 **verkündet** (https://www.republik.ch/2025/05/07/die-schweiz-ist-drauf-und-dran-autoritaere-ueberwachungsstaaten-zu-kopieren): „Die Schweiz ist drauf und dran, totalitäre Überwachungsstaaten zu kopieren."

Selbst wenn man „Bundesbern" zugesteht, die E-ID zum Zwecke der Effizienzsteigerung oder aus sicherheitspolitischen Aspekten einführen zu wollen, rechtfertigen die massiven Risiken nichts anderes als ein klares Nein an der Urne. Denn die E-ID ist unnötig, kostenintensiv und brandgefährlich. Bleibt zu hoffen, dass die Schweizer Stimmbevölkerung von ihrem einzigartigen Privileg Gebrauch macht und auch den zweiten Gesetzentwurf zur E-ID klar ablehnt. Es könnte andernfalls nämlich auch die letzte Entscheidung sein, die die Eidgenossen in Freiheit treffen.

Tom-Oliver Regenauer, Jahrgang 1978, war nach betriebswirtschaftlicher Ausbildung in verschiedenen Branchen und Rollen tätig, unter anderem als Betriebsleiter, Unternehmens- und Management-Berater sowie internationaler Projektmanager mit Einsätzen in

über 20 Ländern. Seit Mitte der 90er-Jahre ist er zudem als Musikproduzent und Texter aktiv und betreibt ein unabhängiges Plattenlabel. Der in Deutschland geborene Autor lebt seit 2009 in der Schweiz. Zuletzt erschienen von ihm „Homo Demens — Texte zu Zeitenwende, Technokratie und Korporatismus“ (2023) und „Truman Show“ (2024). Weitere Informationen unter **regenauer.press** (https://www.regenauer.press/).