

# Die Schweiz ist drauf und dran, autoritäre Überwachungsstaaten zu kopieren

- 07.05.2025
- republik.ch / Republik

Die Vorlage klingt, als wäre sie vom Kreml verfasst worden: Geht es nach dem Bund, müssen sich Schweizer Internetnutzer künftig mit Ausweis oder Telefonnummer identifizieren. Der Zeitpunkt dafür ist denkbar schlecht. Von Adrienne Fichter, 07.05.2025 Teilen Diesen Beitrag anhören 0:00 / 16:05 Selten sorgt eine Verordnung in IT-Kreisen für so viel Aufsehen wie jene zum Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs .

Doch die Verordnung, zu der die Vernehmlassung gestern Dienstag endete, ist auch alles andere als gewöhnlich. Das zeigt sich nicht nur daran, dass der bei Fachleuten sehr angesehene Blog Techradar.com schon vor fünf Wochen warnte, in der Schweiz seien die sichere Verschlüsselung und die Online-Anonymität gefährdet. Sondern auch an einem Schreiben der Kommission für Verkehr und Fernmeldewesen des Nationalrats, die Anfang letzter Woche ein kritisches Schreiben an den Bundesrat schickte. Die Kommission habe Bedenken zum Datenschutz, zu Überregulierung und zur KMU-Belastung, sagt ihr Vizepräsident und SVP-Nationalrat Thomas Hurter auf Anfrage der Republik.

Damit argumentiert Hurter ähnlich wie die Digitale Gesellschaft, die sogar von einem massiven Frontalangriff auf die Grundrechte und die Rechtsstaatlichkeit spricht. Genauso drastische Worte wählt der Chief Operating Officer des welschen Technologie-Start-ups Nym: «In der Schweiz wird es keine private, digitale und datenschutzfreundliche Kommunikation mehr geben», so Alexis Roussel. Und für das erfolgreiche Messenger-Unternehmen Threema ist es sogar denkbar, «wenn nötig» eine Volksinitiative gegen die Verordnung zu lancieren, wie es gegenüber der Republik bestätigt. Ist ihr Ärger angebracht? Stimmt es, dass eine Überwachung droht, wie man sie aus autoritär regierten Staaten kennt? Und: Worum geht es überhaupt? Wichtige Trennung soll aufgehoben werden Wer sich mit Schweizer Überwachungsgesetzen auseinandersetzt, muss sich zuerst durch ein Dickicht von sperrigen Begriffen kämpfen. Die wichtigsten zwei im Zusammenhang mit der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs sind die beiden folgenden: Fernmeldedienstleister: Das sind Unternehmen, die klassische Telekommunikationsdienste für die Öffentlichkeit bereitstellen, etwa Betreiber von Mobilfunk- und Festnetzen wie die Swisscom.

Anbieter abgeleiteter Kommunikationsdienste: Das sind Dienstleister, die Kommunikationsdienste erbringen, ohne eine eigene Fernmeldeinfrastruktur zu betreiben. Dazu zählen Anbieter von Messaging- und E-Mail-Diensten wie beispielsweise Whatsapp oder Signal, aber auch das Non-Profit-Unternehmen Immerda.ch aus Bern, das unter anderem einen E-Mail-Dienst anbietet. Der beim Justizdepartement von SP-Bundesrat Beat Jans angesiedelte Dienst Überwachung Post- und Fernmeldeverkehr legt diese zweite Kategorie in seinem erläuternden Bericht sehr grosszügig aus. So zählt er auch Cloud-Anbieter wie Infomaniak dazu, zudem VPN-Tools und Firmen wie Hostpoint, die Server für das Hosting von Websites zur Verfügung stellen.

Gemäss aktueller Schweizer Rechtslage müssen die Anbieter abgeleiteter Kommunikationsdienste auf Anfrage der Schweizer Strafverfolgung bei verdächtigen Personen alles rausrücken, was sie über sie gespeichert haben. Nicht mehr, nicht weniger. Diese Trennung zwischen Fernmeldedienstleister und Kommunikationsdiensten hatte das Parlament bei der ersten Revision des Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs vor zehn Jahren bewusst eingeführt, um KMU-Unternehmen im Digitalbereich nicht unnötig zu belasten. Der Dienst Überwachung Post- und Fernmeldeverkehr gibt auf Anfrage der Republik zu, dass er nicht viel von der damals beschlossenen Trennung hält. Internetanbieter wie Swisscom und IT-Unternehmen wie Proton, die E-Mail, VPN und auch Dokumentenverwaltung anbieten, sollten künftig denselben Überwachungspflichten unterworfen sein.

Der Überwachungsdienst verkauft diese Neuerung mit dem Argument der Fairness, wenn er schreibt, dadurch werde auch sichergestellt, dass die Anbieter abgeleiteter Kommunikationsdienste «für vergleichbare Dienstleistungen nicht wesentlich geringere Verpflichtungen haben» als die Fernmeldedienstleister. Dies verbessere die Gleichbehandlung. Den ersten Anlauf für eine Revision der Verordnung startete der Dienst bereits während der Pandemie. So veröffentlichte er im Jahr 2022 einen Entwurf, in dem er die Abschaffung der Verschlüsselungen für viele Kommunikationsdienste forderte. Der Paragraph las sich wie eine Schweizer Version der Chatkontrolle: Man musste davon ausgehen, dass eine technische Hintertür bei Messenger-Apps wie Threema eingebaut werden sollte für einen direkten Zugang für Strafverfolgung (wie sie seit Jahren in der EU diskutiert wird).

Ein Aufschrei in den Medien sorgte dafür, dass der Bund diesen umstrittenen Teil verschob und nur den weniger kontroversen Teil in Kraft treten liess. Identifikationspflicht auch für Marktplätze. Mit der aktuellen Teilrevision hat der Bund das alte Verschlüsselungsanliegen erneut aufgenommen. Und legte noch zusätzliche Pflichten obendrauf: Neu müssten viele Schweizer Unternehmen zum Erfüllungsgehilfen des Überwachungsstaats werden. Das Eidgenössische Justizdepartement präsentierte Ende Januar 2025 eine Vorlage, die klang, als wäre sie vom Kreml verfasst worden. Denn praktisch jede Website mit Nachrichtenfunktion wäre von der Vorlage betroffen: Sämtliche digitalen Dienste mit mindestens 5000 Nutzerinnen –egal ob sie E-Mail, Cloud, VPN oder Chat anbieten – müssten diese ausreichend identifizieren und die Daten speichern.

Konkret heisst das: Jede Website, über die sich Personen Direktnachrichten zuschicken können, fiel unter diese Bestimmung. Also beispielsweise auch die Marktplätze Ricardo, Tutti und der Onlinehändler Digitec, schliesslich tauschen sich dort Käufer und Verkäuferinnen aus. Aber auch Videospiel-Betreiber, bei denen sich Gamerinnen über Text- und Videokommunikation austauschen können. Für die Identifizierung müsste eine Ausweis- oder Führerscheinkopie vorgelegt oder zumindest eine Telefonnummer bekannt gegeben werden (die mit der SIM-Karten-Registrierung an eine Ausweiskopie gekoppelt ist). Im erläuternden Bericht des Bundesrats ist auch von einer möglichen Identifikation via Kreditkarte oder Bordkarte auf Flughäfen die Rede, und es wird betont, dass technische Eckdaten wie IP-Adressen nicht ausreichen.

Diese Kundeninformationen müssten alle Unternehmen sechs Monate auf Vorrat speichern. Die St. Galler Strafrechtsprofessorin Monika Simmler bezweifelt, dass diese Vorgaben überhaupt noch dem Bundesgesetz entsprechen. Denn dort ist «von grosser wirtschaftlicher Bedeutung» und «grosser Benutzerschaft» die Rede. «Ich gehe davon aus, dass der Bundesrat seine Kompetenz überschreitet, wenn er bei solch für den Markt unerheblichen Anbietern weiter gehende Pflichten einführt», sagt Simmler.

Anonymität im Internet wäre vorbei. Der Überwachungsdienst behauptet, dass die betroffenen Unternehmen diese Daten ohnehin sammeln. Doch das stimmt nicht: Bisher waren für die Erstellung eines Benutzerkontos auf den entsprechenden Websites kaum Personalien nötig. Jonathan Messmer, der sich für die IT-Anwaltskanzlei Ronzani/Schlauri detailliert mit der Vorlage auseinandergesetzt hat, erklärt: «Wer sagt, die Daten würden «sowieso schon gesammelt», verkennt: Viele Nutzer und Anbieter wollen das gerade nicht – und werden jetzt neu dazu gezwungen.» Mit Anonymität im Internet wäre es komplett vorbei. Sprich: Wer eine Schweizer App, Software oder Plattform nutzt, riskiert, gläsern und identifizierbar zu sein.

Und: KMU müssten einen enormen Aufwand leisten, um jene neuen Datenbanken auch gebührend gegen kriminelle Cyberattacken abzusichern, damit diese nicht im Darknet landen. Dass das möglich sein wird, dürfte eine Illusion sein. Denn Studien aus den letzten Jahren zeigen, dass viele kleine und mittlere Unternehmen das Risiko von Cyberattacken unterschätzen und sich entsprechend zu wenig schützen. Es ist unklar, wie weit der Überwachungsdienst gehen wird, sollte die Verordnung durchkommen. Zwar erwähnt er als Ausnahme explizit Online-Medienportale mit öffentlicher Kommentarfunktion (weil die Leserinnen sich gegenseitig keine Nachrichten schicken können).

Doch die Versprechungen des Bundesrats haben bei diesem Thema eine kurze Halbwertszeit, wie die Entwicklungen der letzten acht Jahre zeigen. Bereits nach der Revision des

Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs im Jahr 2017 liessen die Strafverfolger des Bundes nichts unversucht, um zwei Kommunikationsdienste in eine komplett sachfremde Kategorie hochzustufen: Threema und Protonmail sollten beide als Fernmeldediensteanbieterin eingestuft werden, obwohl beide Firmen nichts mit Internetinfrastruktur zu tun haben und weder über Glasfaserkabel noch Satellitennetzwerke verfügen. Threema und Protonmail hätten als Folge umfassende Überwachungspflichten einführen müssen, etwa eine Echtzeitüberwachung. Beide Unternehmen wehrten sich dagegen vor Gericht. Das Bundesverwaltungsgericht gab Threema im Mai 2020 recht, das Bundesgericht bestätigte dieses Urteil im April 2021.

Protonmail legte ebenfalls beim Bundesverwaltungsgericht erfolgreich Beschwerde ein. Über den Verordnungsweg die Demokratie aushebeln Die Motivation für die Revision der Verordnung liegt damit auf der Hand: Weil die Behörden mit dem Upgrade von Threema und Protonmail juristisch gescheitert sind, gehen die Bundesangestellten nun über den Verordnungsweg, obwohl diese Änderungen sowohl dem Bundesgesetz widersprechen als auch dem Willen des Parlaments, eine Hierarchie von Überwachungspflichten zu haben. Das ist ein demokratiepolitisch höchst fragwürdiges Vorgehen. Mit der neuen Verordnung müssten Unternehmen wie Threema und Proton (das mittlerweile mehr Produkte als nur E-Mail anbietet) ihr auf Datenschutz basierendes Geschäftsmodell aufgeben. Sie wären praktisch den gleichen Pflichten unterworfen wie der Internetkonzern Swisscom, der die Standort- und Telefon-Metadaten seiner Nutzerinnen laufend und für sechs Monate speichert.

Denn die neue Verordnung verlangt, dass neu eine Million Nutzerinnen (global, nicht nur in der Schweiz) oder 100 Millionen Franken Konzernumsatz reichen für das Upgrade und die damit verbundenen «vollen Pflichten». Der Überwachungsdienst verkaufte die Verordnung in einem Gespräch mit Medienschaaffenden als eine Vereinfachung und als KMU-freundliche Revision. Er betonte mehrfach, dass die Revision der Verordnung nicht dazu führe, dass der Überwachungsapparat ausgebaut werde. Der Sprecher des Diensts spielte die Brisanz massiv herunter: «Die meisten Unternehmen werden nie von uns hören und sammeln sowieso schon diese Daten.» Die Revision werde eine Klärung bringen, doppelte der Dienst in einer schriftlichen Antwort an die Republik nach: «Mit der Einführung der neuen «reduzierten Pflichten», welche nur minimale Anforderungen enthalten, wird der Grundsatz der Verhältnismässigkeit künftig besser gewahrt.

» IT-Jurist Messmer lässt dieses Argument nicht gelten: «Neue Pflichten werden eingeführt, bestehende Schwellen drastisch gesenkt und die Privatsphäre im Netz systematisch abgeschafft. Diese Verordnung ist einer der bisher gravierendsten Angriffe auf unsere digitale Freiheit.» Und der Staat wird sehr wohl bald bei Unternehmen anklopfen. Auskünfte mit wenigen Klicks Denn: Alle potenziell betroffenen IT-Unternehmen mit 5000 Nutzerinnen oder Kunden müssen sich bei den Bundesbehörden innert kurzer Frist melden. Versäumen sie dies, droht ihnen eine Busse.

Verlangt eine kantonale Staatsanwaltschaft eine Auskunft, müssen sie diese unter anderem direkt im Verarbeitungssystem des Bundes eingeben. Jonathan Messmer von der IT-Anwaltskanzlei Ronzani/Schlauri sagt: «Im Extremfall könnten Strafverfolgungsbehörden alle fünf Sekunden eine automatisierte Anfrage an Unternehmen mit vollen Überwachungspflichten stellen und somit «in Echtzeit» alle soeben erst registrierten Zugriffe rausholen und eine ganze Historie aufbauen.» Die Schweiz will mit dieser Revision also einen riesigen digitalen Überwachungsapparat bauen, damit die Behörden neu auf Knopfdruck unbegrenzt viele Auskünfte abfragen können. Dass das Volumen bereits heute enorm gross ist, zeigen die letzte Woche vom Überwachungsdienst veröffentlichten Zahlen: Die Kantone und die Bundesbehörden haben doppelt so viele Überwachungsmassnahmen angefordert wie im Vorjahr. Noch mehr Macht für Big Tech Doch nicht nur der Inhalt, sondern auch der Zeitpunkt der Verordnung ist fragwürdig.

So ist am Europäischen Gerichtshof für Menschenrechte in Strassburg eine Klage gegen Vorratsdatenspeicherung hängig, eingereicht von der Digitalen Gesellschaft. Beschwerdeführer sind unter anderem Grünen-Nationalrat Balthasar Glättli und «Beobachter»-Chefredaktor Dominique Strelbel. International lässt sich die Verordnung fast nur mit den drakonischen Internetgesetzen von Russland, China und Iran vergleichen, die entweder eine Realnamenpflicht

oder eine Mobiltelefonnummer für E-Mail, Hosting und alle Arten von digitalen Dienstleistungen verlangen. China fordert etwa Personalien bei der Registrierung für populäre Apps wie Wechat ein. Sollte die Schweiz die neue Cybercrime Convention der Uno ratifizieren, könnten sich jene Diktaturen bei der Strafverfolgung von Dissidentinnen schlimmstenfalls ebenfalls bei den Schweizer KMU bedienen.

Denn diese verlangt eine Zusammenarbeit aller Strafverfolgungsbehörden weltweit. Es ist eine Reform, die nicht nur auf Threema und Proton zielt – zwei der wichtigsten IT-Firmen –, sondern auf unzählige Schweizer Unternehmen, die heute wohl noch gar nichts von diesen Konsequenzen wissen. Die Schweiz sabotiert ihre eigene IT-Industrie damit in einem Moment, wo sie sie am stärksten braucht: in geopolitisch turbulenten Zeiten, in denen die Privacy-Tech-Branche extremen Zulauf erhält und hiesige Cloud-Unternehmen wie Infomaniak auf Plakaten mit «Sichere Schweizer Cloud» werben. Gerade jetzt, wo Bundesbern damit beginnt, sich Gedanken zur digitalen Souveränität zu machen und zur Loslösung von Big-Tech-Konzernen. Und gerade jetzt, wo bereits zwei Kantone ein «Recht auf digitale Integrität» und damit auch Anonymität in ihren Verfassungen verankert haben und in weiteren Kantonen politische Debatten dazu angelaufen sind.

Die Ironie dabei: Mit dieser Verordnung werden amerikanische Big-Tech-Konzerne wie Meta noch mächtiger. Denn für Whatsapp – wie der Sprecher des Diensts Überwachung Post- und Fernmeldeverkehr bestätigt – gelten die Schweizer Gesetze nicht. Teilen Teilen Logo Facebook seit 2018 .