# Der Staat will mehr wissen.

## Die Frage ist nur: Wie viel wollen wir ihm verraten?

### *Die VÜPF und die Frage nach den Grenzen staatlicher Macht*

Wer die Geschichte staatlicher Überwachung studiert, stellt ein erstaunlich konstantes Muster fest. Fast jede neue Befugnis wird mit einem nachvollziehbaren Ziel eingeführt, fast jede neue Datensammlung dient angeblich der Bekämpfung schwerer Kriminalität, fast jede neue Überwachungsmassnahme wird als unverzichtbar dargestellt. Was hingegen deutlich seltener vorkommt, ist die spätere Abschaffung dieser Instrumente. Hat der Staat einmal Zugriff auf bestimmte Daten erhalten, entwickelt sich daraus meist kein Rückbauprogramm, sondern die Grundlage für die nächste Forderung nach zusätzlichen Kompetenzen.

Insofern lohnt sich ein genauer Blick auf die derzeitige Diskussion um die Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, kurz **VÜPF**. Während die einen bereits den Überwachungsstaat vor der Tür sehen und die anderen jede Kritik als Panikmache abtun, geht dabei leicht unter, worum es im Kern überhaupt geht.

## Mehr als eine technische Anpassung

Der Bundesrat präsentierte den ersten Entwurf als notwendige Anpassung an die digitale Realität. Die Kommunikation habe sich verändert, die technischen Möglichkeiten ebenfalls. Messenger-Dienste, E-Mail-Anbieter, VPN-Dienste und andere Kommunikationsplattformen hätten klassische Telefonie und SMS weitgehend verdrängt. Die Strafverfolgung müsse deshalb über Instrumente verfügen, die den neuen technischen Gegebenheiten Rechnung tragen.

Auf den ersten Blick klingt dies nach einer rein technischen Modernisierung. Tatsächlich steckt dahinter jedoch eine Entwicklung, die deutlich älter ist als WhatsApp, Proton oder VPN-Dienste.

Viele Schweizer gehen bis heute davon aus, dass staatliche Überwachung hierzulande nur in Ausnahmefällen stattfindet und die Schweiz im internationalen Vergleich besonders zurückhaltend agiert. Dieses Selbstbild hält einer näheren Betrachtung allerdings nur bedingt stand. Die Überwachung des Fernmeldeverkehrs

ist in der Schweiz seit Jahren gesetzlich geregelt, organisatorisch hoch professionalisiert und technisch eng mit den grossen Telekommunikationsanbietern verzahnt. Wenn Strafverfolgungsbehörden auf Telefonverbindungen, Mobilfunkdaten oder Internetanschlüsse zugreifen wollen, existieren dafür längst etablierte Verfahren und Strukturen.

Wie selbstverständlich diese Realität inzwischen geworden ist, zeigt sich manchmal in den kleinen Erfahrungen des Alltags. Wer schon einmal versucht hat, einen Bluewin-Account bei der Swisscom endgültig löschen zu lassen, dürfte erfahren haben, dass dieser zwar deaktiviert, aber nicht sofort entfernt wird, sondern erst nach Monaten. Offiziell geschieht dies, falls der Kunde seine Meinung doch noch ändern sollte. Eine bemerkenswert fürsorgliche Form der digitalen Nachbetreuung. Der Gedanke, dass Daten auch nach einer Kündigung noch monatelang vorhanden bleiben, wird von den meisten Menschen längst als normal akzeptiert. Dabei zeigt sich hier bereits ein Grundmuster der gesamten Überwachungsdebatte. **Daten werden selten gelöscht, weil sie irgendwann vielleicht noch nützlich sein könnten.** Für den Kunden. Für das Unternehmen. Oder für staatliche Stellen, die später wissen möchten, wer wann mit wem über was kommuniziert hat.

Darin liegt der eigentliche Hintergrund der aktuellen Revision. Der Staat versucht nicht, ein völlig neues Überwachungssystem aufzubauen. Die Infrastruktur existiert bereits. Die gesetzlichen Grundlagen existieren bereits. Die Zusammenarbeit zwischen Behörden und Kommunikationsanbietern existiert bereits. Was sich verändert hat, ist die Kommunikation selbst.

Während klassische Telefonanschlüsse und Internetzugänge seit Jahren Teil dieser Architektur sind, findet ein immer grösserer Teil des digitalen Lebens heute über Messenger-Dienste, verschlüsselte E-Mail-Anbieter, Cloud-Plattformen und VPN-Dienste statt. Bereiche also, die sich der bisherigen Überwachungslogik teilweise entziehen.

> Aus Sicht der Behörden entsteht dadurch eine Lücke, die geschlossen werden soll. Aus Sicht vieler Menschen entsteht damit einer der letzten digitalen Räume, in denen Kommunikation nicht automatisch einer identifizierbaren Person zugeordnet werden kann.

Hier setzt die Revision an. Mit neuen Kategorien von Mitwirkungspflichtigen,

zusätzlichen Identifikationspflichten, neuen Auskunftstypen und erweiterten Aufbewahrungspflichten soll die Nachvollziehbarkeit auch dort sichergestellt werden, wo die bestehende Überwachungsarchitektur an ihre Grenzen stösst.

Für Strafverfolgungsbehörden mag dies wie eine konsequente Modernisierung erscheinen. Für Kritiker stellt sich hingegen eine grundsätzliche Frage: Geht es hier noch um die Anpassung an neue Technologien oder um **die schrittweise Ausdehnung eines Systems, das seit Jahren immer mehr Daten sammelt, immer mehr Personen identifiziert und immer mehr Bereiche des digitalen Lebens erfasst?**

## Eine ungewöhnliche Allianz

Die anschliessende Vernehmlassung brachte ein bemerkenswertes Bild hervor. Anders als bei vielen politischen Vorlagen verlief die Trennlinie nicht entlang der üblichen Parteigrenzen.

Zahlreiche Kantone sowie Fachgremien aus dem Bereich der Strafverfolgung begrüssten die vorgeschlagenen Anpassungen grundsätzlich. Aus ihrer Sicht schliessen die neuen Regelungen bestehende Lücken und erleichtern die Aufklärung von Straftaten.

Auf der anderen Seite formierte sich eine ungewöhnlich breite Allianz aus Technologieunternehmen, Datenschutzorganisationen, Wirtschaftsverbänden und politischen Akteuren unterschiedlichster Couleur. **Unternehmen wie Proton, Threema oder Nym warnten vor erheblichen Eingriffen in die Privatsphäre**, vor negativen Folgen für den Innovationsstandort Schweiz und vor einer Entwicklung, die das Vertrauen in digitale Schweizer Dienstleistungen nachhaltig beschädigen könnte.

Die Diskussion entwickelte sich damit rasch zu weit mehr als einer technischen Debatte über Kommunikationsnetze und Datenbanken.

## Der Ergebnisbericht bestätigt die Kontroverse

Im Februar 2026 veröffentlichte das Eidgenössische Justiz- und Polizeidepartement den Ergebnisbericht zur Vernehmlassung. Wer darin nach einer klaren Siegerseite sucht, wird enttäuscht.

Der Bericht dokumentiert ausführlich die Kritik an Identifikationspflichten, Datenspeicherung, Überwachungsmöglichkeiten, wirtschaftlichen Auswirkungen und datenschutzrechtlichen Risiken. Gleichzeitig hält er fest, dass viele Kantone und Strafverfolgungsbehörden die vorgeschlagenen Anpassungen weiterhin unterstützen.

Die Vorstellung, die Vorlage sei entweder von allen begrüsst oder von allen verworfen worden, hält einer näheren Betrachtung nicht stand. **Vielmehr zeigt sich ein klassischer Zielkonflikt** zwischen dem Wunsch nach wirksamer Strafverfolgung und dem Bedürfnis nach Privatsphäre, Vertraulichkeit und informationeller Selbstbestimmung.

## Die zweite Vernehmlassung: Vieles neu, vieles gleich

Nach der Auswertung der ersten Vernehmlassung kündigte der Bundesrat eine Überarbeitung der Vorlage an. Kritiker hofften auf einen grundlegenden Kurswechsel. Schliesslich hatten Technologieunternehmen, Wirtschaftsverbände, Datenschützer und zahlreiche weitere Organisationen erhebliche Bedenken angemeldet.

Die überarbeitete Vorlage, welche das EJPD am 8. Mai 2026 veröffentlicht hat, liegt inzwischen auf dem Tisch. Wer gehofft hatte, die umstrittensten Elemente würden nach der ersten Vernehmlassung vollständig verschwinden, dürfte beim Lesen überrascht sein.

Zwar wurden einzelne Bestimmungen angepasst, Schwellenwerte verändert und Formulierungen präzisiert. Auch bei der Verschlüsselung reagierte das EJPD sichtbar auf die Kritik. Gleichzeitig bleiben zahlreiche Punkte erhalten, welche bereits in der ersten Vernehmlassung für heftigen Widerstand sorgten.

> Dazu gehören insbesondere Identifikationspflichten, Aufbewahrungspflichten für bestimmte Daten, neue Möglichkeiten zur Benutzeridentifikation sowie zusätzliche Auskunfts- und Überwachungsinstrumente.

Das bedeutet nicht, dass die Kritik wirkungslos geblieben wäre. Es bedeutet aber auch nicht, dass die Vorlage grundlegend neu gedacht wurde.

Wer die erste und die zweite Vernehmlassungsvorlage nebeneinanderlegt, erkennt rasch ein Muster: Über Details wird verhandelt, über die grundsätzliche Richtung nicht. Die Frage lautet eben nicht, ob der Staat zusätzliche Möglichkeiten zur Identifikation und Nachverfolgung digitaler Kommunikation erhalten soll. Diese Richtung steht fest. Diskutiert wird vor allem noch darüber, wie weit diese Möglichkeiten reichen dürfen und welche Anbieter davon betroffen sein sollen.

## Das technische Problem ist in Wahrheit ein politisches

Der Bund beschreibt die Herausforderung als technische Notwendigkeit. Kriminelle nutzen moderne Kommunikationsmittel, Ermittlungen werden komplexer, Identifikationen schwieriger. Daraus ergibt sich aus Sicht der Behörden der Wunsch nach zusätzlichen Informationen.

Diese Darstellung ist nachvollziehbar. Sie beschreibt jedoch nur die halbe Realität.

Denn hinter der technischen Argumentation verbirgt sich eine politische Grundsatzfrage von erheblicher Tragweite. Es geht nicht darum, ob Straftäter verfolgt werden sollen. Darüber herrscht weitgehend Einigkeit. Es geht vielmehr darum, wie viel Freiheit, Anonymität und Privatsphäre eine Gesellschaft bereit ist aufzugeben, damit Ermittlungen einfacher werden.

Diese Frage lässt sich weder durch Informatiker noch durch Juristen allein beantworten. Sie betrifft das Verhältnis zwischen Bürger und Staat und damit einen der sensibelsten Bereiche jeder freiheitlichen Ordnung.

## Warum Grundrechte existieren

Auf den ersten Blick klingt die Forderung nach zusätzlichen Informationen vernünftig. Wer könnte schon etwas dagegen haben, dass Straftaten effizienter verfolgt werden?

Würde die Verbesserung der Strafverfolgung als alleinige Begründung ausreichen, gäbe es kaum einen Grund für das Briefgeheimnis, das Fernmeldegeheimnis, das Arztgeheimnis oder das Anwaltsgeheimnis. Jedes dieser Rechte erschwert staatliche Ermittlungen in gewissem Umfang. Trotzdem wurden sie geschaffen und geschützt, weil freie Gesellschaften erkannt haben, dass nicht jede technisch mögliche Form der Überwachung auch politisch wünschenswert ist.

> Grundrechte wurden nicht erfunden, um Kriminelle zu schützen. Sie wurden geschaffen, um die Grenzen staatlicher Macht festzulegen.

Der Staat ist keine Freundschaftsveranstaltung. Er ist ein Machtapparat mit klar definierten Aufgaben, Kompetenzen und Zwangsmitteln. Genau deshalb wurden in freiheitlichen Gesellschaften Schranken eingezogen, die auch von wohlmeinenden Regierungen nicht beliebig überschritten werden dürfen.

## Die Grenzen der Staatsmacht

Die Diskussion über die VÜPF wird häufig auf einzelne Personen reduziert. Mal steht Beat Jans im Mittelpunkt, mal ein bestimmtes Unternehmen, mal eine Petition. **Damit wird der Blick auf den eigentlichen Kern des Konflikts verstellt.** Es geht nicht um Sympathien für einen Bundesrat und auch nicht um die Frage, ob heutige Behörden verantwortungsvoll handeln. Es geht um die Grenzen staatlicher Macht.

In einem Rechtsstaat werden Grundrechte nicht für den Idealfall geschaffen, sondern für den Ernstfall. Niemand weiss, wer in zehn, zwanzig oder dreissig Jahren politische Verantwortung tragen wird. Niemand weiss, welche Krisen, Konflikte oder gesellschaftlichen Spannungen dann herrschen werden.

Für viele Schweizer hat sich der Blick auf den Staat während der Corona-Jahre grundlegend verändert. Was zuvor für viele eine theoretische Debatte über Kompetenzen, Notrecht und staatliche Eingriffe war, wurde plötzlich zur praktischen Erfahrung. Ausgangsbeschränkungen, Versammlungsverbote, Zertifikatspflichten, Berufsverbote für einzelne Gruppen und ein gesellschaftlicher Druck, wie ihn die Schweiz seit Jahrzehnten nicht mehr erlebt hatte, **zeigten vielen Menschen, wie weit ein Staatsapparat bereit ist zu gehen, wenn er sich auf einen Ausnahmezustand beruft.**

Damals vertrauten viele Menschen darauf, dass aussergewöhnliche Befugnisse nur in extremen Ausnahmefällen eingesetzt würden. Die Erfahrungen jener Jahre haben dieses Vertrauen bei vielen nachhaltig erschüttert. Die zentrale Lehre daraus lautet nicht, dass einzelne Politiker besonders vertrauenswürdig oder besonders gefährlich wären.

> Die zentrale Lehre lautet, dass staatliche Macht dazu neigt, ihre eigenen Grenzen auszutesten, sobald sie sich auf höhere Ziele, Krisen oder ausserordentliche Lagen berufen kann. Was gestern noch als undenkbar galt, kann morgen bereits als alternativlos präsentiert werden.

Wer heute neue Instrumente zur Identifikation, Nachverfolgung und Speicherung von Daten schafft, stellt diese nicht einer einzelnen Person zur Verfügung, sondern dem Staat als Institution. Und Institutionen geben Kompetenzen erfahrungsgemäss nur äusserst selten wieder freiwillig zurück.

Die inzwischen veröffentlichte überarbeitete Vernehmlassungsvorlage zeigt denn auch, dass zahlreiche Kritikpunkte zwar aufgenommen wurden, die grundsätzliche Richtung der Revision jedoch bestehen bleibt. **Identifikationspflichten, Aufbewahrungspflichten und neue Möglichkeiten zur Benutzeridentifikation bilden weiterhin das Fundament der Vorlage.**

Deshalb wird die Diskussion über die VÜPF heute anders geführt als noch vor zehn Jahren. Nicht weil die Menschen plötzlich etwas zu verbergen hätten, sondern weil viele erkannt haben, dass staatliche Befugnisse selten kleiner werden und Krisen häufig als Begründung für zusätzliche Kompetenzen dienen.

Die Debatte über die VÜPF ist deshalb weit mehr als eine Diskussion über technische Standards oder Verwaltungsverordnungen. Sie berührt eine Frage, die jede Generation neu beantworten muss: **Wie viel Wissen soll der Staat über uns besitzen dürfen, damit eine freie Gesellschaft am Ende noch frei bleibt?**

Genau diese Diskussion hätte die Schweiz führen müssen, bevor neue Identifikationspflichten, zusätzliche Datenspeicherung und weitere Überwachungsinstrumente auf den Weg gebracht werden. Stattdessen wurde die Vorlage zunächst als technische Anpassung präsentiert. Doch Technik ist hier nur die Verpackung. Im Kern geht es um Macht, Kontrolle und die Grenzen staatlicher Eingriffe.

Die gute Nachricht lautet: Die Entscheidung ist noch nicht gefallen. Die überarbeitete Vorlage liegt auf dem Tisch. Die politische Diskussion ist nicht beendet und die grundsätzlichen Fragen sind trotz aller juristischen Detailarbeit weiterhin offen.

## Im Kern geht es um Macht.

Dass Behörden mehr Informationen möchten, ist keine Überraschung. Überraschend wäre das Gegenteil.

Entscheidend ist deshalb nicht, was technisch möglich ist, sondern wer darüber entscheidet, welche Möglichkeiten der Staat am Ende auch tatsächlich erhalten soll.

Und hier liegt die politische Brisanz der VÜPF. Die vorgesehenen Änderungen erfolgen auf Verordnungsstufe. **Gegen Verordnungen kann kein Referendum ergriffen werden.** Wer sich dagegen wehren will, ist auf politische Einflussnahme während der Vernehmlassung oder auf spätere gerichtliche Verfahren angewiesen.

Damit verschiebt sich die Debatte aus dem direkten demokratischen Prozess in juristische, administrative und politische Verfahren, die von vielen Bürgern kaum wahrgenommen werden.

Für eine Vorlage, die Identifikationspflichten, Datenspeicherung und neue Möglichkeiten staatlicher Nachverfolgung betrifft, ist das zumindest bemerkenswert.

## Nachgedanke

Vielleicht hat die ganze Diskussion noch eine andere Konsequenz.

Viele Menschen verbringen mehr Zeit damit, den Preis ihres Mobilfunkabos zu vergleichen als sich Gedanken darüber zu machen, wem sie ihre digitale Kommunikation anvertrauen. Dabei ist die Wahl eines E-Mail-Anbieters oft weit mehr als eine Komfort- oder Kostenfrage.

Wer Wert auf Privatsphäre legt, sollte sich nicht nur dafür interessieren, ob ein Dienst kostenlos ist oder über besonders viele Funktionen verfügt. Mindestens ebenso wichtig sind Fragen wie:

- In welchem Land sitzt der Anbieter?
- Welchem Rechtssystem unterliegt er?
- Wo stehen seine Server?
- Wie geht das Unternehmen mit behördlichen Auskunftsersuchen um?
- Und wie transparent informiert es darüber?

Erstaunlicherweise braucht es für diese kleine Recherche oft nicht mehr als ein paar Minuten Zeit und einige Klicks im Internet. Die meisten Anbieter beantworten diese Fragen sogar selbst. Man muss nur aufhören, ausschliesslich auf den Preis zu schauen.

Noch einen Schritt weiter gehen Menschen, die ihre digitale Kommunikation nicht vollständig in die Hände eines einzelnen Anbieters legen möchten. **Eine eigene Domain** kostet heute pro Jahr oft weniger als ein Restaurantbesuch und sorgt dafür, dass die eigene E-Mail-Adresse auch dann bestehen bleibt, wenn man den Anbieter wechselt.

Wer seine Domain bei einem vertrauenswürdigen Hosting-Unternehmen betreibt, gewinnt ein Stück Unabhängigkeit zurück. Statt von den Entscheidungen eines einzelnen Konzerns abhängig zu sein, kann man selbst bestimmen, welchem Anbieter und welchem Rechtsraum man seine digitale Kommunikation anvertrauen möchte.

Absolute Sicherheit gibt es auch damit nicht. Aber digitale Souveränität beginnt häufig mit kleinen Entscheidungen, die man selbst treffen kann. **Die wichtigste davon ist erstaunlich unspektakulär: die Wahl des E-Mail-Anbieters.**