## Willkommen im Land der überwachten Freiheit

# Kabelaufklärung in der Schweiz

**„Willkommen in der Schweiz – dem Land der Freiheit.“ Doch wie frei sind wir wirklich, wenn der Bund weiss, wann wir telefonieren, was wir googeln und wo wir uns gerade aufhalten? Heute schauen wir hinter die Kulissen des perfekten Alpenpanoramas – und sehen, wie die Überwachungsgesellschaft Stück für Stück voranschreitet.“**

## Kabelaufklärung – ein digitales Laubbläser-Paradies

Stellen Sie sich vor, alles, was Sie im Internet tun – Ihre Mails, Chats, Streaming-Dienste und selbst die peinlichen Suchanfragen – wird von einem gigantischen digitalen Laubbläser eingesaugt. Offiziell geht es darum, „nur relevante Daten“ herauszufiltern, um Terroristen und Cyberkriminelle zu stoppen. Doch in der Praxis wird einfach alles gespeichert, was durch die Glasfaserkabel saust.

Der Clou? Wenn Sie in der Schweiz eine E-Mail an Ihre Kollegin schicken, aber der Server im Ausland steht, wird Ihre Kommunikation aufgezeichnet. Der NDB gibt zu, dass es technisch unmöglich ist, solche „Schweiz-via-Ausland-Schweiz“-Kommunikationen in Echtzeit zu erkennen. Erst später, im Zentrum für Elektronische Operationen (ZEO) in Zimmerwald, **wird händisch (!) aussortiert**, was „relevant“ ist – oder auch nicht.

## Die grossen Versprechen und ihre grausame Realität

2016 versprach der damalige Bundesrat: Keine Massenüberwachung! Nur punktuelle Massnahmen gegen Terroristen und andere Bösewichte. Heute zeigt sich, dass diese Zusagen genauso viel Wert hatten wie ein abgelaufener Swiss Travel Pass. Alles wird aufgezeichnet. Warum? Weil es später „nützlich“ sein könnte. Willkommen in der Welt der Retrosuchen, in der der Geheimdienst gespeicherte Daten nachträglich mit neuen Suchkriterien durchleuchtet – natürlich

nur zu Ihrer Sicherheit.

Hier ein paar Highlights der Realität:

- **Massenüberwachung ohne Ausnahme:** Ihre E-Mails, Chats und Suchanfragen – alles landet im Speicher des ZEO.
- **Berufsgeheimnisse adieu:** Ob Journalisten oder Anwälte, niemand kann sich sicher sein, dass vertrauliche Kommunikation nicht mitgelesen wird.
- **Technische Märchen:** Der NDB behauptet, dass rein inländische Kommunikation „geschützt“ sei. Doch in der Realität reisen viele Daten über das Ausland – und sind somit im Überwachungsnetz gefangen.

## Die manuelle Arbeit der Datenschnüffler

Das wirklich Gruselige an der Kabelaufklärung? Sie wird von Menschen durchgeführt, nicht nur von Algorithmen. Die Analysten des ZEO überprüfen die erfassten Datenströme „manuell und inhaltlich detailliert“. Das bedeutet, sie lesen tatsächlich mit. So kann der NDB-Direktor Christian Dussey mit Stolz verkünden, dass seit 2017 keine Kommunikation zwischen Journalisten und deren Quellen „aufgefallen“ sei. Aber um das zu wissen, muss man wohl ziemlich genau hinschauen, oder?

Der Schutz von Journalisten und Anwälten, die sich auf ihre Berufsgeheimnisse verlassen? Ein hübsches Märchen. Sicherheitsinteressen gehen vor – und die Privatsphäre bleibt auf der Strecke.

## Von der Vorratsdatenspeicherung zu Retrosuchen

Neben der Echtzeitüberwachung sammelt der NDB auch munter Daten auf Vorrat. Laut der Digitalen Gesellschaft wird alles, was einmal gescannt wurde, für Retrosuchen gespeichert. Inhalte wie Mails oder Chats bleiben bis zu 18 Monate abrufbar, während Metadaten *(also: Wer hat wann mit wem kommuniziert?)* sogar bis zu fünf Jahre aufbewahrt werden.

Kritiker sprechen von einem „digitalen Heuhaufen“, der immer grösser wird. Der Geheimdienst sucht darin nicht gezielt nach der sprichwörtlichen Nadel, sondern häuft immer mehr Heu an. Vielleicht stolpert man ja irgendwann zufällig über etwas Brauchbares.

# Die Geheimhaltung – eine Blackbox voller Überraschungen

Die genauen technischen Details der Kabelaufklärung sind streng geheim. Klar ist aber, dass der NDB komplette Glasfaserkabel *(auf OSI Layer 2)* abgreift. Das bedeutet, dass der gesamte Datenstrom kopiert wird – ohne Rücksicht darauf, ob die Kommunikation schützenswert ist oder nicht. Schon der Abgriff selbst stellt einen massiven Eingriff in die Privatsphäre dar.

Die Zusammenarbeit mit den Telekommunikationsanbietern wie Swisscom, Sunrise und Salt ist gesetzlich vorgeschrieben. Diese Unternehmen müssen dem NDB Zugang zu ihrer Infrastruktur gewähren, dürfen aber keine Details preisgeben. Auch kleinere Anbieter werden zunehmend in die Überwachung einbezogen.

# Ein Überwachungsstaat unter dem Deckmantel der Demokratie

Während die Bevölkerung in Sicherheit gewiegt wird, dass die Überwachung nur „gezielt“ erfolgt, zeigt sich ein ganz anderes Bild. Der Geheimdienst baut seine Kapazitäten ständig aus. Selbst Glasfaserkabel ausländischer Anbieter sind im Visier des NDB. Kleinere Unternehmen erhalten Anweisungen, wie und wo Daten abgegriffen werden sollen, während grosse Anbieter ihre Schweigepflicht wahren müssen.

### Politische und rechtliche Konsequenzen

Die Digitale Gesellschaft kämpft seit Jahren juristisch gegen die Kabelaufklärung. Doch trotz aller Bemühungen scheint die Politik mehr daran interessiert, bestehende Überwachungspraktiken nachträglich zu legalisieren. Die geplante Revision, die eine Erweiterung der Überwachungsbefugnisse des Nachrichtendienstes des Bundes (NDB) vorsieht, ist noch nicht abgeschlossen.

Aktueller Stand der Revision**:**

- Aufteilung der Revision in zwei Teile: Aufgrund einer Administrativuntersuchung zur Informationsbeschaffung durch den Bereich Cyber des NDB wurde die Revisionsvorlage in zwei Teile aufgeteilt.

- Erster Teil *(„Revision Grundpaket“)*: Dieser Teil, der sich bereits 2022 in der Vernehmlassung befand, soll bis Ende 2025 vom Bundesrat zuhanden des Parlaments verabschiedet werden. Ein Inkrafttreten wäre somit frühestens 2027 möglich.
- Zweiter Teil *(„Revision Cyber“)*: Für diesen Teil ist eine ergänzende Vernehmlassung bis Juli 2025 geplant. Die genaue Zeitplanung für die weitere Behandlung und ein mögliches Inkrafttreten stehen noch nicht fest.

## Neue Perspektiven im Datenaustausch mit den USA?

Das neue Swiss-US Data Privacy Framework wird als Datenschutz-Meilenstein verkauft, doch die Realität sieht anders aus: Die Schweizer Geheimdienste nutzen seit Jahren Auswertungsprogramme aus den USA, und der Datenaustausch lief über geheime Kanäle ohnehin weiter. Die angebliche „Rechtssicherheit“ ist nur ein Feigenblatt, während unsere Daten nach Übersee wandern. Wer an „angemessenen Datenschutz“ glaubt, darf sich freuen: Verkauft wird Transparenz, geliefert wird totale Überwachung.

## Fazit: Die Schweiz – ein Überwachungsstaat im Schafspelz

Die Kabelaufklärung zeigt, dass die Schweiz längst den Weg zum gläsernen Bürger eingeschlagen hat. Unter dem Vorwand der Sicherheit wird die Privatsphäre der Bevölkerung systematisch ausgehöhlt. Die versprochene Balance zwischen Sicherheit und Freiheit? Ein schlechter Witz.

Wenn wir nicht jetzt handeln, könnte die Schweiz bald zu einem digitalen Überwachungsparadies werden – mit uns allen als gläsernen Bürgern. Willkommen in der Schweiz, dem Land der scheinbaren Freiheit und der unsichtbaren Gitterstäbe.