Der Bund überwacht uns alle

Vor der Abstimmung zum Nachrichtendienstgesetz versprach der Bundesrat: Eine flächendeckende Überwachung der Bevölkerung wird es nicht geben. Doch heute ist die Kabelaufklärung genau das: ein Programm zur Massenüberwachung. Die Serie zum Schweizer Überwachungsstaat, Folge 1.

Von Adrienne Fichter (Text) und Erik Carter (Animation), 09.01.2024

Als im Juni 2013 der britische «Guardian» die Aussagen von Edward Snowden publik machte, stand die Welt für einen Moment still. Die Enthüllungen von Snowden, seines Zeichens Ex-Dienstleister des US-amerikanischen Auslandsgeheimdienstes NSA, bestätigten die schlimmsten Befürchtungen: Die amerikanischen Geheimdienste lesen nach Belieben mit, wie wir über E-Mail kommunizieren oder nach welchen Begriffen wir suchen. Sie wissen Bescheid über unsere Ängste, unsere Träume und Wünsche, über unsere intimsten Geheimnisse. Snowden konnte diese Massenüberwachung umfangreich dokumentieren. Seither wird er von den USA wegen Verstosses gegen den «Espionage Act» per Haftbefehl gesucht. Er lebt in Moskau im Exil.

In den Jahren darauf haben Geheimdienste anderer Länder diese Überwachungspraxis kopiert, die Regierungen haben sie in nationale Gesetze gegossen. So auch die Schweiz. Der Abstimmungskampf rund um die Revision des Nachrichtendienstgesetzes im Jahr 2016 fiel heftig aus. Die Juso, die Grünen, die SP und die Piratenpartei fuhren schweres Geschütz auf, redeten vom «Schnüffelstaat» und von «Mini-NSA». Manche Gegnerinnen der Gesetzesrevision warnten gar vor einem Fichenstaat 2.0.

Die umstrittenste Änderung betraf die sogenannte «Kabelaufklärung». Es ist genau jene Methode, die Snowden bei der NSA publik gemacht hatte: die Überwachung der Kommunikation über Internet-Kabelnetze im Auftrag des Nachrichtendiensts. Dabei wird die Kommunikation standardmässig nach bestimmten Suchbegriffen – oder sogenannten «Selektoren»- – durchsucht: Das können etwa spezifische Informationen zu ausländischen Personen oder Firmen sein, Telefonnummern beispielsweise, es können auch Bezeichnungen für Waffensysteme oder Technologien sein. Wird ein Begriff gefunden, wird die entsprechende Nachricht an das ZEO weitergeleitet, das Zentrum elektronische Operationen des Verteidigungsdepartements, das in der Berner Gemeinde Zimmerwald beheimatet ist.

Die Analysten des ZEO wandeln diese Signale, die auf unterschiedliche Weise verschlüsselt sein können, nach Möglichkeit in lesbare Kommunikationsdaten um – und leiten diese dann je nach Ergebnis an den Nachrichtendienst weiter. Das Ziel: Informationsbeschaffung, etwa für die Spionage- und Terrorismusabwehr, Schutz der Landes- und Sicherheits-

interessen, aber auch Austausch von Informationen mit befreundeten Geheimdiensten.

Die Versprechen

Die Vorstellung, dass der Nachrichtendienst des Bundes (NDB) wie die amerikanische NSA alle Chats und E-Mails, alle Suchanfragen und abgerufenen Videos einfach mitlesen und -schauen könnte, war für viele Schweizerinnen erschreckend. Darum beschwichtigten die Behörden im Abstimmungskampf und auch danach immer wieder:

- Eine Massenüberwachung wie in anderen Ländern sei nicht vorgesehen, sagte Guy Parmelin, der damalige Vorsteher des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS), im Sommer 2016.
- Mit Kabelaufklärung würden keine Schweizer Bürger überwacht – weder im In- noch im Ausland, beteuerte NDB-Sprecherin Isabelle Graber eine Woche vor der Abstimmung.
- Der damalige Nachrichtendienstchef Markus Seiler weibelte persönlich für das Gesetz. Nachdem es angenommen worden war, versicherte auch er: «Es wird keine Massenüberwachung geben.»
- Die neuen Regelungen zur Kabelaufklärung seien «so eng gefasst, dass dieses Mittel nur gegen konkrete Bedrohungen eingesetzt werden kann und eine flächendeckende Überwachung aller Bürgerinnen und Bürger ausgeschlossen ist», betonte der Bundesrat im Abstimmungsbüchlein.
- Bereits in der Botschaft zum Nachrichtendienstgesetz von 2014 hatte der Bundesrat argumentiert, Kabelaufklärung sei ein «Mittel der Auslandsaufklärung», bei dem sich «die Zielobjekte» – also die zu überwachenden Personen – «im Ausland befinden».

Die Realität

Diese Recherche zeigt, dass kein einziges dieser Versprechen eingehalten wurde. Exklusive Dokumente – Gerichtsakten und amtliche Korrespondenz –, die der Republik vorliegen, verschaffen erstmals Einblick in das Vorgehen des Nachrichtendiensts bei der Kabelaufklärung. Sie zeigen:

1. Seit Inkrafttreten des Gesetzes 2017 wird der Internetverkehr von Schweizerinnen massenhaft mitgelesen. In gerichtlichen Dokumenten räumt das Verteidigungsdepartement ein, dass **die «inländische» Kommunikation inhaltlich gelesen und ausgewertet** werde. Und: Sämtliche Daten werden für spätere Auftragssuchen gespeichert.
2. Eine Konsequenz daraus: Journalisten können den Quellenschutz technisch genauso wenig gewährleisten wie Anwältinnen das Anwaltsgeheimnis. Denn das Cyberzentrum ZEO und der Nachrichtendienst **schützen jene Berufsgruppen explizit nicht** – und darum wird deren Kommunikation unter Umständen an den Nachrichtendienst weitergeleitet.
3. 2023 hat der Nachrichtendienst gar **Schritte unternommen, um die Kabelaufklärung weiter auszubauen.** Kleinere Unternehmen erhielten eine Aufforderung, ihre Infrastruktur für die Überwachung durch den Dienst ZEO vorzubereiten.
4. Der Nachrichtendienst und das ZEO **gehen für das Anzapfen der Kabel** direkt auf Schweizer Unternehmen zu, die selber gar keinen grenzüberschreitenden Datenverkehr anbieten. Dieses Vorgehen steht im Widerspruch zu den Beteuerungen des Nachrichtendiensts, wonach nur Anbieter mit grenzüberschreitenden Leitungen angezapft würden.

Digitale Gesellschaft versus Schweizer Nachrichtendienst

Schauen wir erst einmal zurück. Das Verdikt war eindeutig: Am 25. September 2016 nahm die Schweizer Stimmbevölkerung das revidierte Nachrichtendienstgesetz mit 65,5 Prozent Ja-Stimmen an. Doch für den Verein Digitale Gesellschaft war das Thema damit nicht vom Tisch. Denn er war überzeugt, dass die Beschwichtigungen des Bundesrats rund um die Kabelaufklärung nicht der Wahrheit entsprachen. Schon im Vorfeld der Abstimmung hatten sich die Aktivistinnen deshalb mit Journalisten und Anwältinnen vernetzt, die dann später als Beschwerdeführerinnen auftreten sollten. Warum gerade sie? Weil sie zur Ausübung ihres Jobs sensitive Informationen über digitale Kanäle austauschen – und berufliche Pflichten haben: Sie müssen ihre Quellen schützen und das Berufsgeheimnis gegenüber Dritten einhalten.

Gemeinsam mit ihnen bereitete die Digitale Gesellschaft ein Gesuch vor, das sie just auf den Tag des Inkrafttretens des neuen Gesetzes am 1. September 2017 beim Nachrichtendienst einreichten. Die Beschwerdeführer forderten, dass der Nachrichtendienst in ihren Fällen keine Kabelaufklärung anwenden dürfe. Denn dies stelle eine Verletzung ihrer Grundrechte dar. Sie beriefen sich auf die Rechte der Europäischen Menschenrechtskonvention, auf das Berufsgeheimnis und den Quellenschutz.

Wie erwartet lehnte der Nachrichtendienst das Gesuch postwendend ab. Die Allianz zog den Fall weiter, reichte 2018 Beschwerde beim Bundesverwaltungsgericht ein. Dieses wies die Beschwerde im Jahr darauf ab. Die Richter erachteten das im Gesetz vorgesehene Auskunftsrecht – also die Möglichkeit, beim Nachrichtendienst nachzufragen, ob persönliche Daten beim Geheimdienst gespeichert sind – als «Rechtsschutzmöglichkeit, die wirksamen Grundrechtsschutz sicherzustellen vermag». Kurz: als ausreichend.

Die Digitale Gesellschaft sah dies anders. Die Aktivistinnen zogen den Fall an das Bundesgericht weiter.

Dort kam es zur überraschenden Kehrtwende: Die Bundesrichter hielten am 1. Dezember 2020 fest, dass das grundsätzliche Auskunftsrecht keinen wirksamen Schutz gegen Überwachung darstelle. Sie rügten zudem das Bundesverwaltungsgericht, weil sich dieses nicht inhaltlich mit der Beschwerde auseinandergesetzt hatte. Die Vorinstanz musste nun also vertieft prüfen: Werden die Grundrechte der sieben Aktivistinnen, Journalisten und Anwältinnen verletzt?

Was folgte, war eine seit drei Jahren andauernde Auseinandersetzung zwischen allen involvierten Parteien – der Beschwerdeallianz, dem Nachrichtendienst und dem Bundesverwaltungsgericht – rund um die Frage:

Wie genau funktioniert die Kabelaufklärung in der Schweiz?

Es ist eine Frage, die der Nachrichtendienst nur widerwillig und stückchenweise beantwortet. Und das hat Gründe. Aus der Korrespondenz zwischen den verschiedenen Parteien, die der Republik vollständig vorliegt, geht klar hervor: Die Datenströme von Bürgerinnen aus der Schweiz fliessen massenhaft nach Zimmerwald zum Zentrum elektronische Operationen. Denn die Kabelaufklärung wird auf Chats, E-Mails und Suchanfragen jeder einzelnen Person angewandt, die in der Schweiz lebt.

Das «Schweizer Internet» und die «Faser nach Syrien»

Widmen wir uns erst einmal der Frage: Welche Kabel werden überwacht? In einer Stellungnahme zuhanden des Bundesverwaltungsgerichts schreibt der Nachrichtendienst, dass «nur diejenigen physischen Verbindungen» ausgewählt würden, welche «grenzüberschreitenden Datenverkehr (...) aus einer für einen bestimmten Kabelaufklärungsauftrag relevanten Region enthalten». Der Nachrichtendienst behauptet also: Ein Abgriff finde nur auf jenen Kabeln statt, die die Schweiz mit dem Ausland verbinden. Er sagt damit, er sei in der Lage, jene Fasern zu erkennen, über die beispielsweise zwischen der Schweiz und Syrien kommuniziert wird. Er registriere, wenn etwa auf «einer Faser viel Verkehr auf Syrien durchläuft. Diese Faser wird dann weiterbearbeitet.»

Auf Anfrage der Republik hin wird diese Behauptung wiederholt und als Beleg eine Grafik geschickt, die zeigen soll, wie der Dienst «nur Fasern des Kabels» auswählt, die «Kommunikation aus einer bestimmten Region» wie Syrien oder dem Irak enthalten.

Bild

Die Grafik des NDB findet sich auch in diesem Dokument auf Seite 24.Bodara

In der Korrespondenz mit der Digitalen Gesellschaft betont der Geheimdienst mehrfach, eine «rein inländische Kommunikation» (zum Beispiel von Genf nach St. Gallen) werde gar nicht erfasst. Der Kommunikationsverkehr zwischen zwei Personen aus der Schweiz erfolge innerhalb der Landesgrenzen: «Das Internet schickt in der Regel die Pakete über den kürzesten Weg an die Destination», heisst es in einem Schreiben des Nachrichtendiensts.

Diese Erklärungen zur Funktionsweise des Internets sind mehr als fragwürdig: Sie sind objektiv falsch. Und sie offenbaren ein höchst abenteuerliches Verständnis von der Funktionsweise des Internets.

Beginnen wir mit der «Faser nach Syrien». Fredy Künzler, Netzwerkingenieur und Geschäftsführer von Init7, einem Internetanbieter aus Winterthur, erklärt: «Das Internet-Routing ‹von/nach Syrien› ist keineswegs eine statische Kabelverbindung, sondern kann permanent ändern.»

Die globale Routing-Tabelle – also die Informationen, aufgrund deren die Datenpakete zur Zieladresse geleitet werden – ändert laufend. Die Behauptung des Nachrichtendiensts, er könne Fasern mit viel Verkehr zwischen zwei bestimmten Destinationen erkennen, widerspricht der Funktionsweise des Border Gateway Protocol – des Routingprotokolls, mit dem im Internet verschiedene Anbieterinnen zusammengeschaltet werden.

Welcher Pfad für den Datenaustausch der Beste ist, ermittelt das Border Gateway Protocol nämlich automatisch anhand verschiedener Parameter wie Verfügbarkeit, betriebswirtschaftliche Abwägungen oder der Kapazitätsauslastung. Interessanterweise räumt dies der Nachrichtendienst in seinem erläuternden Bericht zu einer derzeit geplanten Revision des Nachrichtendienstgesetzes selber ein. Dort heisst es nämlich: «Die internationalen Datenströme werden über hochdynamische Netzwerke geleitet, deren Routing sich rasch ändern und nicht langfristig vorausgesagt werden kann.»

Damit sind wir beim zweiten Punkt, dem «Schweizer Internet». Auch die Aussage, dass Datenpakete in der Regel den kürzesten Weg neh-

men, stimmt schlicht nicht. Schon allein deshalb nicht, weil die Schweizer Internetanbieter unterschiedlich untereinander verbunden sind. Nicht alle möchten mit allen «peeren», also Datenpakete austauschen. Das führt dazu, dass Datenpakete von A nach B nicht nur in Ausnahmefällen, sondern in der Regel via Ausland geroutet werden – und die Daten über die Landesgrenze und wieder zurück fliessen. In den Worten von Netzwerkingenieur Künzler: «Die Idee eines Schweizer Netzes ist eine Illusion.»

Ein paar wenige Beispiele machen das deutlich: Wenn jemand aus der Schweiz eine im Ausland gehostete Website wie beispielsweise www.nytimes.com aufruft, fliessen Daten über die Grenze. Auch die Mailserver verschiedener Internetanbieter stehen in EU-Ländern, jene von Sunrise und von UPC Hispeed etwa in Österreich und den Niederlanden. Eine Nutzerin, die ihre UPC-Mails in der Schweiz abruft und von dort versendet, schickt standardmässig Datenpakete über die Landesgrenze und erhält solche zurück. Viele Schweizer Unternehmen nutzen zudem für die interne Kommunikation amerikanische Tools wie Slack. Auch hier erfolgt bei jeder Nachricht zwischen Angestellten eine «Migration» der Datenpakete über die Landesgrenzen, hin und zurück.

Eine breite Datenautobahn

Der Nachrichtendienst räumt in seinen Stellungnahmen selbst ein, dass es nicht möglich ist, den Datenverkehr zwischen Kommunikationsteilnehmerinnen in der Schweiz von vornherein auszusieben. So schreibt er, dass die Kommunikation zwischen einem Sender und einer Empfängerin in der Schweiz, die über das Ausland läuft, bei der Kabelaufklärung erfasst werde. Auf Anfrage bestätigt der Nachrichtendienst: «Sogenannte ‹Schweiz-via-Ausland-Schweiz›-Kommunikationen bereits während dem Senden zu erkennen, ist technisch unmöglich (...).» Erst bei der Sichtung der Daten in Zimmerwald könne es erkannt werden, falls «aus Versehen» digitale Kommunikation und Internetnutzung von Einwohnern der Schweiz mitgeschnitten worden sei, schreibt er sinngemäss in einem der Dokumente.

Damit wird zum einen schwarz auf weiss widerlegt, was der ehemalige Nachrichtendienstchef Markus Seiler am 14. Juni 2016 gegenüber dem «Bund» behauptete: Die Kabelaufklärung komme «nicht zum Einsatz, wenn sich zwei Schweizer via eine von einem ausländischen Anbieter betriebene Mail-Adresse unterhalten».

Stattdessen belegen die Ausführungen, was die Digitale Gesellschaft bereits 2019 konstatierte: Das ZEO führt eine Massenüberwachung durch.

Journalistinnen und Anwälte ungeschützt

Zum anderen wird ebenfalls klar: Die Analystinnen des ZEO prüfen die ausgeleiteten Datenströme manuell und inhaltlich detailliert. Heisst: Sie lesen alles mit. So schreibt der Geheimdienst, dass das Cyberzentrum in Zimmerwald eine «inhaltliche Prüfung der Suchresultate auf Schweizbezug» durchführe. Dass der Datenstrom genauestens geprüft wird, ist auch an einer anderen Stelle belegt. Ironischerweise ausgerechnet dort, wo es um den Quellenschutz von Journalistinnen geht: Der seit 2022 amtierende NDB-Direktor Christian Dussey versichert in einem Schreiben an das Bundesverwaltungsgericht, dass seit 2017 in keinem der Suchresultate eine Kommunikation zwischen einem Journalisten und seiner Quelle erkannt worden sei.

Im (doch eher beunruhigenden) Umkehrschluss kann konstatiert werden: Die Analysten müssen ziemlich genau wissen, was in den herausgesiebten Chats oder Mails geschrieben steht, um eine solche Aussage machen zu können. Das bestätigt auch Dussey im Schreiben: «Hinweise auf eine konventionsrechtlich geschützte Person können weder in der Funk- noch in der Kabelaufklärung automatisiert erkannt werden. Vielmehr bedarf es der manuellen Arbeit der Analystinnen und Analysten.»

Sollten die VBS-Analystinnen bei der Auswertung auf eine Kommunikation zwischen Medienschaffenden und ihren potenziellen Quellen stossen, «würde das ZEO die betreffenden Daten unter Berücksichtigung der Verhältnismässigkeit nur an den NDB weiterleiten, wenn dies zur Abwehr einer konkreten Bedrohung notwendig ist bzw. auf Anweisung des NDB die Daten löschen», schreibt Dussey. Auch hiermit bestätigt der NDB-Direktor, dass die Sicherheitsinteressen gegenüber dem journalistischen Quellenschutz priorisiert werden – und dieser faktisch aufgehoben ist.

Medienschaffende und Anwälte müssen also generell davon ausgehen, dass ihre Kommunikation mit Klientinnen und Quellen zu jedem Zeitpunkt nach Zimmerwald ausgeleitet werden kann – und je nach Interpretation ihres Inhalts auch an den Nachrichtendienst weitergereicht wird.

«Retrosuchen» im Heuhaufen

Dieser Befund ist gerade deshalb brisant, weil der Nachrichtendienst gegenüber der Digitalen Gesellschaft schriftlich einräumt, dass die nach Zimmerwald ausgeleiteten Daten – Chats, Mails und Suchanfragen oder einfach sehr persönliche Daten – dort auch gespeichert werden. Dies erlaubt es dem Geheimdienst, sogenannte «Retrosuchen» durchzuführen, wie er Ende 2022 in einer Stellungnahme eingeräumt hat: Es läge «in der Natur eines Kabelaufklärungsauftrags, dass sich bestimmte erfasste Signale und Daten erst im Nachhinein als auftragsrelevant herausstellen».

Was die Speicherdauer angeht, so verweist die Nachrichtendienstsprecherin Isabelle Graber gegenüber der Republik auf die Verordnung über den Nachrichtendienst. In dieser ist festgehalten, dass alle vom ZEO erfassten Kommunikationsdaten spätestens nach 18 Monaten gelöscht werden, die erfassten Verbindungsdaten (also die Metadaten, die angeben, wer mit wem über welchen Kanal kommuniziert hat) nach 5 Jahren.

Der Geschäftsführer der Digitalen Gesellschaft und Informatiker Erik Schönenberger glaubt: «Alles, was schon einmal inhaltlich gescannt wurde, wird wohl für die ‹Retrosuche› aufbewahrt.» Der Schweizer Geheimdienst macht also genau das, was in der parlamentarischen Beratung des Gesetzes im Jahr 2015 von den Grünen und den Grünliberalen befürchtet worden ist: Er sucht nicht gezielt nach der Nadel im Heuhaufen, sondern schichtet immer mehr Heu auf. Und die Analystinnen graben sich in mühseliger Fleissarbeit durch den sich immer höher türmenden Heustock hindurch.

Die genauen Analysemethoden des Zentrums elektronische Operationen – also welche Informationen dabei mit welchen Mitteln gewonnen werden – bleiben eine Blackbox. Zurzeit sucht das ZEO Softwareingenieure für den Bau einer Plattform für die «Verarbeitung und Analyse» von abgefangenen zivilen Kommunikationsdaten.

Ausbau der Überwachung

Ebenfalls keine Auskunft gibt der Nachrichtendienst zur Frage, welche der Schweizer Telecomkonzerne und Internetanbieter bei der Kabelaufklärung mitmachen müssen – jene Unternehmen also, welche die Kabelinfrastruktur für das Internet in der Schweiz betreiben. Klar ist: Die drei Grossen, Sunrise, Swisscom und Salt, fallen alle unter die Pflicht der Kabelaufklärung, wie sie auf Anfrage bestätigen. Die Telecomkonzerne verweisen aber ebenfalls darauf, dass ihnen per Gesetz nicht erlaubt sei, über die Umsetzung der Kabelaufklärung zu sprechen.

Die Recherchen der Republik zeigen: Im Jahr 2023 hat der Nachrichtendienst Schritte unternommen, um die Kabelaufklärung auszuweiten. Mehrere kleine Internetanbieter haben Post erhalten aus Zimmerwald. Auch Fredy Künzler von Init7 erhielt vor zwei Monaten per eingeschriebenen Brief einen «Fragebogen» aus Zimmerwald. Wobei es sich dabei vielmehr um einen Befehl des Nachrichtendiensts handelte, Angaben über die technische Infrastruktur zu machen.

Die schriftlichen Fragen geben auch Aufschluss darüber, wie der Nachrichtendienst die Überwachung technisch einrichtet. Internetanbieter wie Init7 müssen darlegen, wie ein Teil ihrer Signale ausgekoppelt wird. Und sie müssen die Frage beantworten, ob die Datenpakete auf ihren Routern in Echtzeit kopiert werden können. Das ZEO will zudem wissen, wie der Zutritt zu den Daten- und Rechenzentren geregelt ist und ob es in den Räumen, in denen sich diese befinden, ihre Anzapfgeräte aufstellen könne, wofür sie Serverschränke und Strom benötige.

«Die Informationen über die Netzinfrastruktur werden benötigt, um den bestmöglichen Abgriffspunkt zu bestimmen und somit die richtigen Signale am richtigen Ort auszuleiten», erklärt NDB-Sprecherin Isabelle Graber auf Anfrage der Republik.

Doch der NDB hat seine Netze im Jahr 2023 noch weiter ausgeworfen: So interessiert sich der Geheimdienst auch für die Glasfaserkabel ausländischer Internetdienste. Zurzeit sind mehrere entsprechende Verfahren vor Gericht hängig. Ein Schweizer Infrastrukturanbieter wehrt sich vor dem Bundesverwaltungsgericht gegen eine Verfügung aus Zimmerwald, in der das ZEO verlangt, die Leitungen von dessen ausländischen Kunden ohne deren Wissen anzapfen zu dürfen.

Aus den Informationen geht klar hervor: Das Zentrum elektronische Operationen des Verteidigungsdepartements schreibt nicht die ausländischen Unternehmen an, welche die grenzüberschreitenden Kabelleitungen betreiben. Sondern direkt die Schweizer Firmen, die mit diesen Kunden verbunden sind, selber aber gar nicht über grenzüberschreitende Leitungen verfügen. Dieses Vorgehen steht im Widerspruch zu den Beteuerungen des Geheimdiensts. NDB-Sprecherin Isabelle Graber wiederholt auf Anfrage: «Nur Provider, die öffentliche Leistungen im Sinne des Fernmeldegesetzes (FMG) im grenzüberschreitenden Verkehr anbieten, können verpflichtet werden.» Doch das ist zum Beispiel im Fall des erwähnten Schweizer Infrastrukturanbieters nicht der Fall.

«Der NDB überschreitet seine Kompetenzen»

Kritiker der Kabelaufklärung fühlen sich durch die Rechercheergebnisse der Republik bestätigt. SP-Nationalrat Fabian Molina hatte sich als damaliger Juso-Präsident im Abstimmungskampf stark engagiert. Für ihn ist mit

der Recherche nun klar, «dass die damaligen Informationen des Bundesrats nicht korrekt waren. Die Grundrechte der Schweizer Bürgerinnen und Bürger werden massiv verletzt.» Die Daten könnten auch in die falschen Hände geraten. «Das muss politisch aufgearbeitet werden. Der NDB überschreitet offensichtlich seine Kompetenzen.»

Auch der grüne Nationalrat, ehemalige Bundesratskandidat und IT-Unternehmer Gerhard Andrey zeigt sich wenig überrascht. Er weist darauf hin, dass die Grünen bereits 2015 bei der parlamentarischen Beratung des Nachrichtendienstgesetzes beantragt hätten, «den ganzen Abschnitt zur Kabelaufklärung zu streichen». Schon damals sei klar gewesen, dass auch der Internetverkehr mit Ziel und Quelle in der Schweiz überwacht werden würde.

Die Zusicherung des damaligen Bundesrats Ueli Maurer, der im Jahr 2015 noch VBS-Vorsteher war, sei schon damals «nachweislich falsch» gewesen, sagt Andrey – Maurer sagte im Wortlaut: «Kabelaufklärung ist dann möglich, wenn einer der Partner im Ausland ist, nicht dann, wenn beide in der Schweiz sind und die Kommunikation über einen ausländischen Server geht. Einer der Betroffenen muss im Ausland sein.»

Wird die Praxis nun legalisiert?

Das vorläufige Fazit: Politiker haben 2016 falsche Tatsachen vorgegaukelt. Die Aussage des früheren VBS-Vorstehers Guy Parmelin, es werde keine Massenüberwachung geben, war nachweislich falsch. Unser Internetverkehr wird gescannt und ausgewertet. Die Schweiz steht anderen Ländern wie etwa Deutschland in nichts nach, das mit dem BND-Gesetz in den letzten Jahren dieselbe Praxis legalisiert hat und bis zu 30 Prozent der Internetkommunikation weltweit anzapft.

2024 wird sich entscheiden, ob es zu einem Ausbau oder zu einer Eindämmung dieser staatlichen Überwachung kommt. Denn es steht nicht nur der Entscheid des Bundesverwaltungsgerichts zur Kabelaufklärung an. Das VBS plant auch eine erneute Revision des Nachrichtendienstgesetzes.

Einen ersten Anlauf dafür nahm es bereits im Jahr 2022. In dieser Vorlage war unter anderem eine Ausdehnung der Kabelaufklärung auf Schweizerinnen vorgesehen, die sich im Ausland befinden. In der Vernehmlassung dazu hagelte es jedoch so viel Kritik aus der Zivilgesellschaft, dass das VBS nochmals über die Bücher ging. Im ersten Halbjahr 2024 ist nun der nächste Anlauf geplant, wie der NDB auf Anfrage bestätigt. Die Antwort des Bundesrats in einer Antwort auf die Interpellation der grünen Nationalrätin Marionna Schlatter kurz vor Weihnachten lässt die Stossrichtung des zweiten Versuchs erahnen: Bisher nicht rechtmässige Datennutzungen durch den NDB sollen neu legalisiert werden.

Was genau in der neuen Vorlage drinstehen wird, ist noch unklar. Beobachterinnen gehen davon aus, dass die geplante Ausweitung der Kabelaufklärung auf weitere Personen auch im neuen Entwurf drinbleiben wird.

Damit würde nachträglich legalisiert, was de facto längst geschieht. Denn dass die Kabelaufklärung gezielt auf einzelne Personen angewendet werden kann, war nie mehr als ein Mythos. De facto ist sie: ein Programm zur Massenüberwachung der in der Schweiz lebenden Bevölkerung.

Die Korrespondenz zwischen der Digitalen Gesellschaft, dem Bundesverwaltungsgericht und dem Nachrichtendienst wurde am heutigen 9. Januar 2024 auf der Website der Digitalen Gesellschaft vollständig publiziert.

Veranstaltung: Der Schweizer Staat, das Internet und du

Am Dienstag, 23. Januar diskutieren wir in Zürich darüber, wie wir zunehmend überwacht werden. Mit dabei sind Viktor Györffy, Anwalt in verschiedenen Verfahren für die Digitale Gesellschaft, Janik Besendorf, Digital Security Lab von «Reporter ohne Grenzen», und Adrienne Fichter, Tech-Reporterin und Autorin der Serie «Surveillance fédérale». Alle Informationen zu dieser Veranstaltung finden Sie hier.