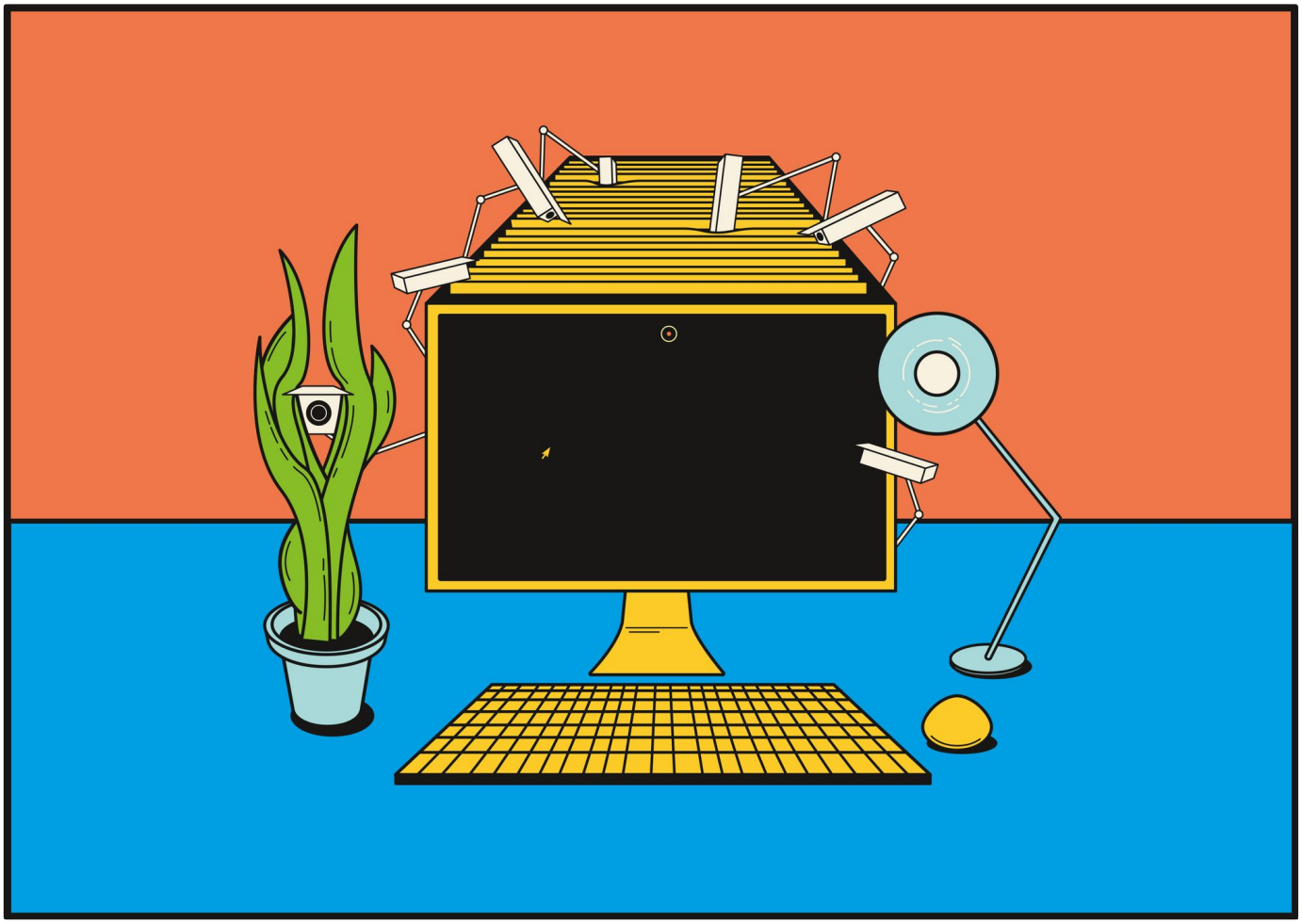


Fischzüge des Überwachungsstaats

Schweizer Sicherheitsbehörden haben in den letzten Jahren grossen Datenappetit entwickelt – zum Leidwesen von Internetfirmen wie dem Messenger-Dienst Threema. Mit dem neuen Anti-Terror-Gesetz nähme der Hunger weiter zu.

Von Adrienne Fichter (Text) und Matthias Seifarth (Illustration), 26.05.2021

Am 13. Juni kommt das Anti-Terror-Gesetz zur Abstimmung. Damit sollen die Kompetenzen der Polizei bei der Überwachung potenzieller Täter ausgeweitet werden. Das sorgt für kontroverse Diskussionen. Vergessen geht dabei manchmal, dass in der Schweiz schon seit Jahren ein Gesetz gilt, das Strafverfolgungsbehörden viele Kompetenzen einräumt: das «Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs», kurz: Büpf.

Das Büpf wurde 2000 in Kraft gesetzt und erfuhr am 1. März 2018 ein digitales Update. Es gibt Strafverfolgerinnen Rechte und Instrumente in die

Hand, um im Datenstrom von Telekomunternehmen gezielt nach Personen und Daten zu suchen.

Seither haben die Informationsanfragen bei Telekomunternehmen und Internetfirmen massiv zugenommen. Sie richten sich an Firmen wie Swisscom oder Sunrise, aber auch an Internet-KMU wie den Mailanbieter Protonmail oder den Messenger Threema. Diese wehren sich zunehmend juristisch gegen die behördliche Praxis – aus Sorge um die Privatsphäre ihrer Kunden und weil die Informationsanfragen zunehmend Kosten verursachen.

Und weil sie befürchten: Wird nach dem Büpf auch das Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus in Kraft gesetzt, nimmt der staatliche Überwachungsaktionismus noch mehr zu.

Grosser Aufwand für kleine Firmen

Seit den Snowden-Enthüllungen von 2013 ist klar: Das Internet ist permanent unsicher. Ob E-Mail oder Facebook-Nachrichten, potenziell kann der amerikanische Auslandgeheimdienst NSA alle Datenströme anzapfen. Daher haben sich neue Firmen auf Verschlüsselungen von Kommunikationsdiensten spezialisiert. Threema und Protonmail sind zwei Start-ups, die einen Messenger und ein E-Mail-Programm entwickelt haben, welche verschlüsselte Nachrichten senden können.

Die Unternehmen profitieren von ihrer «Swissness» – und den jüngsten Entwicklungen in der Big-Tech-Welt. So sind die Downloads der App Threema geradezu explodiert, nachdem Facebook die Verknüpfung seiner Nutzerprofile mit dem Tochterunternehmen Whatsapp bekannt gegeben hatte. Und auch Protonmail betont, man habe vom Bedürfnis nach abgesicherter Kommunikation während Homeoffice-Zeiten profitiert.

Doch beide Firmen haben in der Schweiz zunehmend ein Standortproblem. Und das hat mit dem bereits erwähnten Büpf zu tun.

Vor 2018, in den «guten alten Zeiten», wie sie Threema-Chef Martin Blatter nennt, mussten kantonale Staatsanwältinnen sogenannte «Editionsverfügungen» an Firmen richten, um Datenauskünfte zu erhalten – also eingeschriebene Briefe mit ihren Forderungen. Tage konnten verstreichen, bis die Auskunft erteilt wurde. Waren die formellen Anforderungen für Auskunftsgesuche nicht erfüllt, war es für die Firmen ein Leichtes, diese abzulehnen.

Doch dieser aus Sicht der Strafverfolger schwerfällige Prozess ist Geschichte, seit das revidierte Büpf in Kraft ist. Heute kann eine Kantonspolizistin oder ein Staatsanwalt eine Auskunft elektronisch über den sogenannten Dienst ÜPF («Überwachung Post- und Fernmeldeverkehr») verlangen und sollte innerhalb weniger Stunden eine Antwort erhalten. Die angefragte Firma erfährt dabei weder, um welches Delikt es sich handeln könnte, noch, wer Absender der Anfrage ist: kantonale Strafverfolgerinnen, das Bundesamt für Polizei (Fedpol), der Nachrichtendienst des Bundes, die Bundesanwaltschaft.

Eine Auskunft – also die Identifizierung von Personen – wird mit 3 Franken entschädigt, obwohl der Aufwand dafür mindestens 30 Minuten beträgt, wie verschiedene Unternehmen erklären. Behörden erfahren also die Namen und bestenfalls Telefonnummern von Zielpersonen für sehr wenig Geld. «Das macht es für Strafverfolger besonders attraktiv, auch für Bagatelldelikte Daten zu sammeln», sagt ein betroffener Unternehmer.

Die Höhe der Gebühr wird derzeit neu diskutiert, weil Fredy Künzler, Gründer des Telekomunternehmens Init 7, erfolgreich gegen eine Verfügung des Dienstes ÜPF geklagt hat. Der Dienst hat das Urteil angefochten, der Fall liegt beim Bundesgericht. Solange dessen Entscheid nicht vorliegt, bleiben die Abfragen billig.

Weite Netze werden ausgeworfen

Viele Firmen mutmassen: Gerade weil es so kostengünstig ist, grasen Schweizer Behörden Kontaktlisten zunehmend ziellos und in exzessivem Umfang ab. Die Zahlen, welche die Unternehmen dazu ausweisen, stützen diese Vermutung.

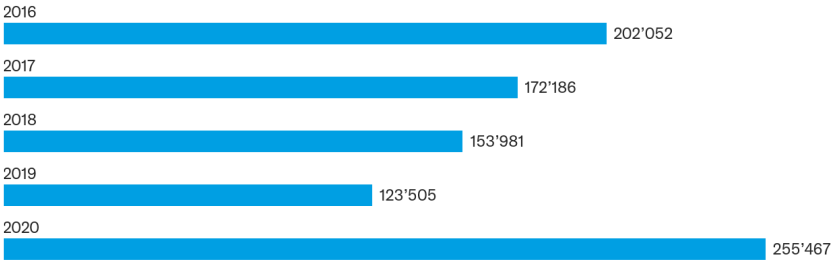
- 3426 Informationsanfragen gingen 2020 beim E-Mail-Service-Provider Protonmail ein, wie Sprecher Edward Shone sagt. Das sind mehr als doppelt so viele wie 2019, wie ein Abgleich mit dem firmeneigenen Transparenzbericht zeigt. Grund dafür sei das revidierte Büpf. «Bis Mitte 2019 war es ruhig», sagt Firmenjurist Mark Loebekken. «Man merkte, dass der Staat Zeit brauchte, um die technischen Systeme für die Datenauskünfte zu entwickeln. Doch dann explodierte es.»
- Eine ähnliche Dynamik zeigt sich bei Threema. 2018 wurden nur 28 Gesuche für personenbezogene Auskünfte an die Firma gerichtet. 2020 waren es über 100. Pro Gesuch verlangen die Behörden im Schnitt die Daten von 5 Personen. In einem Fall wurden sogar die Daten von 44 Personen angefragt. «Man gibt den Behörden den Finger, und sie wollen die ganze Hand», kritisiert Threema-Chef Martin Blatter.
- Stark betroffen ist auch der verschlüsselte Messenger-Dienst Wire. Dessen Server stehen zwar in Deutschland, juristischer Sitz ist jedoch die Schweiz. Gemäss seinem Transparenzbericht erhielt Wire 2018 nur eine einzige Anfrage für eine Datenauskunft. 2019 waren es 192 und 2020 schliesslich 349.

Aus der offiziellen Statistik zum ÜPF geht hervor: Sehr oft stecken das Fedpol und der Nachrichtendienst des Bundes hinter diesen sogenannten «einfachen Anfragen». 2020 hat alleine das Fedpol rund 115'000 dieser Anfragen an Firmen gerichtet – also etwa nachgefragt, welcher Name zu einer Mobilnummer gehört, wer sich hinter einer IP-Adresse verbirgt oder wer eine gewisse Messenger-ID hat. 2019 waren es noch 15'000 Anfragen gewesen, also nur ein Achtel.

Die Gesamtzahl aller Anfragen hat sich von 2019 auf 2020 verdoppelt. Zuvor hatten sich die Behörden zurückgehalten. Dies, weil sie in der Handhabung des Systems erst ausgebildet werden mussten, wie Jean-Louis Biberstein vom Dienst ÜPF sagt. Nach der Einführung automatisierter und standardisierter Abfragen 2019 stiegt die Zahl jedoch auf ein Rekordhoch.

So viele Anfragen wie noch nie

Anzahl «einfacher» Auskünfte des ÜPF



Quelle: ÜPF.

Eine weitere Anfrageart betrifft die Metadaten der digitalen Kommunikation, sie heisst «IR COM». Die Behörden wollen dabei von einer Firma alle Informationen erhalten, die irgendwie verfügbar sind. Relevant ist das etwa für Firmen mit datenschutzorientierten Geschäftsmodellen wie Threema. Die Firma muss dann herausrücken, mit wem eine Userin kommuniziert hat.

«Stösst die Polizei bei Ermittlungen auf Hinweise, dass Kriminelle mit Messenger-Apps kommunizieren, sind IR-COM-Anfragen eine Möglichkeit, um mehr über die Personen herauszufinden, beispielsweise hinterlegte E-Mail-Adressen», bestätigt Fedpol-Sprecher Florian Näf. Auch die Zahl der IR-COM-Anfragen hat sich von 2019 auf 2020 verdoppelt: von 764 auf 1425.

Der Nachrichtendienst des Bundes will diese Zunahme nicht kommentieren. Das ist heikel: Die Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten kritisiert den NDB in ihrem neuesten Bericht im Bereich Datenbearbeitung. Es sei nicht klar, weshalb und welche personenbezogenen Informationen in den Datenbanken gesammelt würden.

Nils Güggi, Sprecher des Dienstes ÜPF, erklärt das Anfragevolumen mit den Schwierigkeiten der Tätersuche: «Ich kann mir sehr gut vorstellen, dass zur Identifikation eines Täters oder einer Täterin die Abfrage mehrerer Nutzerprofile nötig ist.»

Büpf-Anfragen werden zum Streitfall vor Gericht

Genau gegen diese Mehrfach-Abfragen hat sich Threema diesen Februar gewehrt. Der Messenger-Dienst hat dem Dienst ÜPF einen Brief geschrieben. Darin schreibt Threema: Gemäss Artikel 22 des Büpf sollten Internet-Unternehmen nur Auskünfte zur Identifizierung einer einzigen Person ausliefern – nicht mehrerer.

Der Dienst ÜPF antwortete prompt. Threema müsse gemäss besagtem Artikel sämtliche Daten zum Netzwerk eines Täters liefern: «Dies erfasst auch Informationen aus dem Umfeld der Täterschaft.» Das Schreiben beruft sich ausserdem auf Artikel 15. Darin ist die Rede von der Bestimmung von «Personen sowie der mit diesen in Verbindung stehenden Personen».

Im Brief, der der Republik vorliegt, steht ausserdem ein mahnender Satz, keinen grossen Widerstand gegen die Begehren des Überwachungsdiensts zu leisten: «Eine Infragestellung oder Überprüfung von Auskunftsgesuchen durch die Mitwirkungspflichtigen ist im Gesetz auch nicht vorgesehen.»

Die Frage, welcher Gesetzesartikel – 15 oder 22 – zum Zuge kommt, weist auf einen weiteren Konflikt hin, der zwischen Threema und dem Dienst ÜPF schwelte. Dabei ging es um die Deutungshoheit darüber, in welcher Kategorie der Messenger eingestuft wird. Für den Überwachungsdienst ist klar: Threema mit seinem 20-köpfigen Team soll die gleichen Pflichten wie grosse Telekomunternehmen haben, trotz unterschiedlichem Geschäftsmodell.

Dies hat sich Threema nicht so vorgestellt. Ähnlich wie Protonmail und weitere kleine Firmen war man bei der Revision des Büpf der Auffassung, künftig als «abgeleiteter Dienst» zu gelten. Also als Dienstleister, der kein eigenes Netz betreibt, sondern auf einem bestehenden Netz aufbaut und deshalb deutlich weniger umfangreiche Überwachungspflichten hat.

Doch rund einen Monat nachdem das revidierte Büpf in Kraft getreten war, publizierte der Dienst ÜPF ein Merkblatt. Darin steht, internetbasierte Dienste wie Messenger und Netzwerke seien funktional gleichzusetzen mit den «Fernmeldediensten», also mit Netzbetreibern wie Swisscom oder Sunrise. Das heisst unter anderem auch, dass sie Daten darüber, welche Nutzerin mit wem auf welche Weise kommuniziert hat, 6 Monate lang speichern müssen.

Im Dezember 2018 flatterte bei Threema eine Verfügung ins Haus. Der Dienst ÜPF ordnete an, dass das Schwyzer Start-up eine Echtzeitüberwachung einführen und ausserdem die Verschlüsselung der Metadaten (also die Informationen: Wer chattet mit wem?) entfernen müsse.

Simon Schlauri, Anwalt von Threema, erachtete diese Forderungen als unhaltbar. In den Beratungen des Büpf in National- und Ständerat habe von links bis rechts ein Konsens bestanden, dass Kommunikationsdienste wie Threema als «abgeleitete Dienste» keine Echtzeitüberwachung leisten müssten, weil dies ihnen existenzgefährdende Kosten aufbürden würde. Auch der Bundesrat habe dies in seiner Botschaft so geschrieben. Zudem würde der Dienst ÜPF seine Kompetenzen überschreiten, so Schlauri: Er dürfe nicht eigenmächtig entscheiden, welche Firmen in welche Kategorie fallen würden. Dies könne nur der Bundesrat.

Die Argumentation überzeugte offenbar zunächst auch die Richter des Bundesverwaltungsgerichts, die eine Beschwerde von Threema 2020 gutgeheissen haben. Der Dienst ÜPF zog das Urteil jedoch weiter und ignorierte in der Zwischenzeit das Verdikt. Er listete in der soeben publizierten Statistik Threema weiter als «Fernmeldeanbieter» auf. Zu Unrecht, wie das Bundesgericht nun entschied: Am 17. Mai wiesen die Bundesrichter die Beschwerde ab und hielten fest: Threema ist keine Fernmeldeanbieterin.

Ein Achtungserfolg für das Innerschweizer Start-up, mit potenzieller Signalwirkung für Firmen mit Verschlüsselungen als Kerngeschäft.

Der Sieg dürfte auch Protonmail Auftrieb geben. Der Genfer Firma drohte dasselbe Schicksal wie Threema. Auch sie wurde als Fernmeldeanbieter eingestuft. Protonmail legte ebenfalls Beschwerde ein beim Bundesverwaltungsgericht und plant ausserdem eine Aktion, in der sie die National- und Ständerätinnen für die Überwachungsthematik sensibilisieren will.

Ich will es genauer wissen: Wie der Dienst ÜPF seine Kompetenzen kontinuierlich ausweitete

Dass die Bundesbehörden ihre Überwachungskompetenzen ausreizen, hat Tradition. Der Dienst ÜPF wollte bereits 2011 Zugriff auf die Internetdaten von Smartphone-Besitzerinnen im Sunrise- und Swisscom-Handynetz erhalten. Sunrise wehrte sich dagegen: Die Mobilnetzüberwachung sei weder im damals geltenden Gesetz noch in einer Verordnung erwähnt. Das Bundesgericht bestätigte diesen Befund und pfiff den Dienst ÜPF zurück.

Erfolgreicher war die Behörde beim sogenannten Antennensuchlauf, also bei einer Informationsabfrage zu allen Smartphones, die mit einer bestimmten Mobilfunkantenne während eines bestimmten Zeitraums verbunden waren. Auch dieser war im Büpf nicht erwähnt. Doch der Dienst ÜPF führte die Massnahme klammheimlich ein. Erst im Nachhinein hiess das Bundesgericht die Praxis 2011 gut. Schliesslich wurde der Begriff Antennensuchlauf über die Verordnung – genannt Vüpf – integriert.

Auch aktuell versucht der Dienst ÜPF seine Befugnisse weiter auszuweiten – über ein sachfremdes Gesetz. Im Gesetz über «Administrative Erleichterungen und die Entlastung des Bundeshaushalts» möchte der Bund die Bearbeitung von Kontakt-, Kommunikations- und Bewegungsprofilen auf Grundlage der anlasslosen und verdachtsunabhängigen Vorratsdatenspeicherung legalisieren, wie die Digitale Gesellschaft kritisiert. Die Vorlage liegt derzeit bei der Kommission für Verkehr und Fernmeldewesen.

Doch weshalb sind die Sicherheitsbehörden so erpicht darauf, immer mehr Nutzerinformationen von datensparsamen Internet-Start-ups wie Threema zu sammeln?

Antworten darauf liefert die allgemeine Entwicklung des globalen Internets und die sogenannte Echtzeitüberwachung – eine der zugelassenen Prozeduren im Rahmen des Büpf. Die Behörden werden damit ermächtigt, den Internetverkehr einer verdächtigen Person vollständig zu überwachen. Nach Genehmigung durch ein Zwangsmassnahmengericht etwa soll einem Verdächtigten in der Theorie beim Surfen quasi über die Schulter geschaut werden: vom Artikel der NZZ über den aufgesuchten Wetterbericht bis zur Google-Eingabe «Wie baue ich eine Bombe?».

In der Praxis wird diese Möglichkeit den Behörden zunehmend verwehrt. Aus technischen Gründen: Die meisten Browser wie Chrome und Firefox unterstützen seit einigen Jahren nur noch verschlüsselte Webseiten (man erkennt diese am Adresszusatz «https»). Das bedeutet: Die Strafverfolgerinnen sehen die Metadaten (zum Beispiel die URL nzz.ch), aber nicht die Inhalte, die überwachte Personen sich auf einer Webseite ansehen (also den konkreten NZZ-Artikel).

Kriminelle verlagern zudem ihre Kommunikation zunehmend in sichere, verschlüsselte Kanäle, wie Fedpol-Sprecher Florian Näf bestätigt. Und das macht Threema für die Behörden interessant. Sie drängen vermehrt auf Meta-Informationen, wie zum Beispiel hinterlegte Telefonnummern.

Threema-Chef Martin Blatter kritisiert dieses Vorgehen als wenig sinnvoll.

Wer sich beim Dienst anmeldet, hat die Wahl: Er kann sich mit seiner Mobilnummer registrieren oder anonym ein Profil anlegen. «Ein Krimineller wird den anonymen Weg wählen», meint Blatter. «Er will ja keine Spuren hinterlassen.» Überdies kenne Threema die wahren Telefonnummern und E-Mail-Adressen ohnehin nicht – man habe nur eine gehashte, also algorithmisch anonymisierte Version gespeichert. Bei einer Mehrheit der Anfragen könne man daher sowieso nichts Brauchbares liefern.

Anti-Terror-Gesetz würde auch Messenger-Apps treffen

Die zunehmende Verschlüsselung des Internets war ursprünglich auch der Anlass für die Revision des Büpf, schreibt der Jurist Thomas Hansjakob im Grundlagenwerk «Überwachungsrecht der Schweiz». Um diese zu knacken, brauche es sogenannte *government software,* Govware genannt. Dabei handelt es sich um aufwendige Programme, die – installiert auf dem Smartphone – die eintreffenden Nachrichten abfangen und an den Staat weiterleiten, noch bevor die Verschlüsselung passiert. Kantone verfügen über eine solche Software, um Messenger-Apps zu knacken, im Volksmund heisst sie: Staatstrojaner.

Solche Govware kam 2020 genau 13 Mal zum Einsatz. Anlass dafür waren gemäss ÜPF-Statistik Tätigkeiten von kriminellen Organisationen, Verstösse gegen das Betäubungsmittelgesetz und Geldwäscherei.

Künftig könnten die Anwendung von Trojanern und die Datenabfragen via ÜPF zunehmen. Wird am 13. Juni das Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus angenommen, so würde sich das in der Überwachungsstatistik des Diensts ÜPF niederschlagen. Die im PMT-Gesetz behandelten Themen kämen nämlich neben Straftaten wie Diebstahl oder Drogenhandel als weitere Delikt-Kategorie hinzu. Dies bestätigt Jean-Louis Biberstein vom Dienst ÜPF.

Wie diese Kategorie genau heissen wird, ist noch unklar. «Das Anti-Terror-Gesetz muss als Grund für Überwachungen und Abfragen transparent ausgewiesen werden», sagt Jean-Louis Biberstein.

Dies hätte auch Konsequenzen für die Digital-Start-ups. Sie müssten aufgrund der zusätzlichen Polizeikompetenzen im Bereich der Terrorismusprävention wohl mit einer noch grösseren Anfrageflut rechnen. Dabei ist diese schon heute kaum zu bewältigen: «Wir helfen gerne bei der Bekämpfung schwerer Kriminalität mit», sagt Threema-Chef Martin Blatter. «Doch die Überwachung droht zurzeit endgültig aus dem Ruder zu laufen.»

Zuspruch erhalten die Start-ups von der ehemaligen SP-Ständerätin Anita Fetz. «Der Aufwand wird die junge Digital- und Internetindustrie stark behindern», sagt sie. Den Nutzen der Abfragen halte sie demgegenüber für gering. «Leider ist der Zeitgeist im Moment voll auf die vermeintliche Sicherheit ausgerichtet.»

FDP-Ständerat Thierry Burkart, ein Befürworter des Anti-Terror-Gesetzes, glaubt hingegen nicht, dass dieses zu mehr Überwachungen führen wird. «Gemäss Angaben des EJPD ist von ungefähr 30 Personen pro Jahr auszugehen, die meisten davon sind irgendwo bereits erfasst und werden bereits überwacht.»

Fakt ist: Viele Kantone wenden bereits heute algorithmusbasierte Prognosetools an, um mutmassliche Gefährderinnen von morgen zu erfassen. Kantonale Polizeigesetze ermächtigen die Behörden, bei häuslicher Gewalt präventiv einzugreifen. Und mit dem neuen Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus wird der Begriff der «Gefährder» noch einmal deutlich ausgeweitet.

Wo Strassburg das letzte Wort hat

Das neue Büpf ist seit drei Jahren in Kraft. Seine Auswirkungen werden zunehmend spürbar: Behörden entwickeln einen immer grösseren Datenhunger, Trojaner kommen zum Einsatz, Bürgerdaten werden mit wenigen Klicks geliefert. Dies beeinträchtigt nicht nur die Privatsphäre, sondern stellt auch die Standortstrategie des Bundes infrage. Der Bundesrat möchte ähnlich wie die EU eine ethische Digitalisierung mit Fokus auf Datenschutz fördern.

Ob die Schweiz auf dem eingeschlagenen Weg weitermachen kann, ist offen. Das Bundesgericht hat 2018 eine Klage abgewiesen, die sich grundsätzlich gegen die Vorratsdatenspeicherung gerichtet hatte – also dagegen, dass Telekomfirmen die Verbindungsdaten ihrer Nutzerinnen 6 Monate lang aufbewahren müssen, damit Behörden im Bedarfsfall darauf zugreifen können. Beschwerdeführerin war unter anderem die Digitale Gesellschaft.

Sie hat sich darauf an die höchste für die Schweiz zuständige Instanz gewendet: den Europäischen Gerichtshof für Menschenrechte in Strassburg.

Ihre Erfolgschancen stehen gar nicht so schlecht. Mehrere andere Gerichte in Europa – das deutsche Verfassungsgericht, der Europäische Gerichtshof in Luxemburg und das belgische Verfassungsgericht – haben ähnlich lautende Klagen gegen die Vorratsdatenspeicherung zuletzt gutgeheissen.

Das letzte Wort darüber, was die Schweizer Strafverfolgungsbehörden im Internet tun dürfen, ist also noch nicht gesprochen.