Peyrot, Schlegel & Györffy
Rechtsanwälte

Zürich, 19. Oktober 2022

Viktor Györffy
Rechtsanwalt
Beethovenstrasse 47
8002 Zürich
Telefon 044 240 20 55
Telefax 043 500 55 71
gyoerffy@psg-law.ch
www.psg-law.ch

Einschreiben
Bundesverwaltungsgericht
Abteilung I
Postfach

9023 St. Gallen

Digitale Gesellschaft, … / Nachrichtendienst des Bundes NDB
Geschäfts-Nr. A-6444/2020

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

In der eingangs erwähnten Angelegenheit beziehe ich mich auf Ihre Verfügung vom 19. August 2022 und reiche Ihnen innert der entgegenkommenderweise erstreckten Frist zur Stellungnahme des Beschwerdegegners vom 18. August 2022 folgende Stellungnahme ein:

1. Der Beschwerdegegner bringt sinngemäss vor, es gehe im gegenwärtigen Stadium des Verfahrens einzig um die Feststellung, wie Funk- und Kabelaufklärung funktioniere (Ziff. 10 der Stellungnahme des Beschwerdegegners vom 18. August 2022). Es sei verständlich, dass die Beschwerdeführenden gerne wissen möchten, welche Internet-Provider welchen leitungsgebundenen, grenzüberschreitenden Fernmeldeverkehr an den durchführenden Dienst übergeben. Doch erstens sei diese Information geheim (Art. 43 Abs. 3 NDG, auch zum Schutz dieser Provider) und zweitens sei diese Information für das vorliegende Verfahren belanglos (Ziff. 11 der Stellungnahme). Das «Narrativ» der Beschwerdeführenden drehe sich primär um die Fragen, wie effektiv die Funk- und Kabelaufklärung im Einzelfall sei und ob sie als Massnahme sinnvoll sei. Letztere Frage müsse der Gesetzgeber beantworten, erstere Frage sei Bestandteil der Prüfung durch das Bundesverwaltungsgericht anlässlich der Beurteilung der Erst- und Verlängerungsanträge des Beschwerdegegners sowie durch die unabhängige Kontrollinstanz gemäss Art. 79 NDG. Es ziele daher an der Sache vorbei, wenn die Beschwerdeführenden sich nicht nur über das angeblich illegale Verhalten der Vorinstanz ausliessen, sondern sogar dem Bundesverwaltungsgericht schlampige Arbeit unterstellten (Ziff. 12 der Stellungnahme).

2. Dazu ist in grundsätzlicher Hinsicht Folgendes festzuhalten: Die Vorbringen der Beschwerdeführenden werden mit den Ausführungen des Beschwerdegegners unrichtig und unvollständig wiedergegeben. Ebenso wird damit die Prüfung, welche das Bundesverwaltungsgericht gemäss Rückweisungsentscheid des Bundesgerichts und gemäss Rechtsprechung des EGMR vorzunehmen hat, unzutreffend referiert.

3. Die Funk- und Kabelaufklärung setzt an der bestehenden, auf Funkwellen bzw. Kabel beruhenden Kommunikationsinfrastruktur an. Wie die Funk- und Kabelaufklärung funktioniert, wie effektiv sie ist, wie viel und wessen Kommunikation von diesen Massenüberwachungsprogrammen wie direkt betroffen ist, hängt von der bestehenden Kommunikationsinfrastruktur ab, von der Art und Weise, wie Kommunikation durch die Funk- und Kabelaufklärung abgegriffen und ausgewertet wird und welche Arten von Kommunikation davon betroffen sind. Die geforderte effektive Überprüfung des Systems der Funk- und Kabelaufklärung, einschliesslich der Vollzugspraxis und der Effektivität der vorgesehenen Kontrollmechanismen, bedingt eine zureichende Untersuchung dieser technischen Gegebenheiten und Zusammenhänge. Nur wenn diese Gegebenheiten und Zusammenhänge im Beschwerdeverfahren erhoben und für die Beschwerdeführenden nachvollziehbar gemacht werden, ist zu ermessen, mit welchen Eingriffen in die Grundrechte die Funk- und Kabelaufklärung in der Praxis verbunden sind und inwieweit die bestehenden Kontrollmechanismen diese Massenüberwachungsprogramme effektiv einzugrenzen sowie einen Missbrauch der Überwachungsbefugnisse zu verhindern vermögen.

4. Die Relevanz der technischen Gegebenheiten, welche den Möglichkeiten und der Effektivität der Funk- und Kabelaufklärung Limiten setzen, zeigt sich auch in den Darlegungen der Parteien dieses Beschwerdeverfahrens. Nicht nur die Beschwerdeführenden, sondern auch der Beschwerdegegner hat ausführliche Darlegungen zur Funktionsweise der Funk- und Kabelaufklärung und der damit im Zusammenhang stehenden Kommunikationsinfrastruktur gemacht. Die Vorbringen des Beschwerdegegners erscheinen allerdings über weite Teile nicht als akkurat, sondern als schwammig, schlecht verständlich und mit den technischen Gegebenheiten nicht als vereinbar.

5. Mit Darlegungen und fiktiven Beispielen, welche keine Klarheit zu schaffen vermögen und stattdessen Fragen aufwerfen, weil sie in technischer Hinsicht nicht als akkurat und stellenweise schlechterdings als unverständlich erscheinen, kann der Beschwerdegegner keinen Beitrag zur effektiven Überprüfung des Systems der Funk- und Kabelaufklärung leisten. Der Beschwerdegegner vermag auf diese Weise auch nicht wie von ihm geltend gemacht zu belegen, dass die Funk- und Kabelaufklärung grundrechtskonform sei.

6 In seiner Stellungnahme liefert der Beschwerdegegner erneut Erklärungen, wie er bei der Funk- und Kabelaufklärung vorgehe, um damit die Darlegungen der Beschwerdeführenden zu kontern. Nach wie vor ist aber zu konstatieren, dass das, was der Beschwerdegegner vorbringt, über weite Strecken als unklar oder schlichtweg als falsch erscheint.

7. Der Beschwerdegegner macht in seiner Stellungnahme erneute Ausführungen dazu, wie er eruieren könne, dass grenzüberschreitender Datenverkehr vorliege und wie er Kommunikation ausfiltern könne, wenn sich sowohl Sender als auch Empfänger der Kommunikation in der Schweiz befinden (Ziff. 35 ff. der Stellungnahme). Die Ausführungen beziehen sich insbesondere auf serverbasierte Kommunikation. Der Beschwerdegegner schreibt, es komme nicht häufig vor, dass ein Benutzer in der Schweiz zwar mit einem anderen Benutzer in der Schweiz kommuniziere, er sich hierzu aber eines ausländischen Servers als Relais bediene. Schon praktisch gar nicht würden hierfür Server in jenen Regionen der Welt benutzt, für welche die Kabelaufklärung genehmigt worden ist. Die Kommunikation von Personen in der Schweiz mit anderen Personen in der Schweiz bleibe im Regelfall in der Schweiz. Aus Effizienzgründen hätten die Internet-Provider kein Interesse daran, den Datenverkehr über das Ausland umzuleiten. Wer von Basel nach Zürich fahren wolle, nehme die direkte Strecke und nicht jene der Deutschen Bahn über Schaffhausen (Ziff. 38 f. der Stellungnahme).

8. Dazu ist Folgendes zu bemerken: Wie schon mehrfach dargelegt, ist serverbasierte Kommunikation alles andere als eine Ausnahme, ebenso wenig ist es selten, dass dabei die Kommunikation von einem Teilnehmer in der Schweiz zu einem oder über einen Server im Ausland geht. Es sei dazu auch auf die nachstehenden Ausführungen zu Serverstandorten und deren IP verwiesen.

9. Der Beschwerdegegner insistiert in diesem Zusammenhang darauf, dass grenzüberschreitender Datenverkehr vorliege, wenn ein Kommunikationsteilnehmer aus der Schweiz beim Surfen oder beim Versenden von Emails mit Servern im Ausland kommuniziere (Ziff. 37 u. 40 der Stellungnahme). Zwar ist richtig, dass es sich in diesem Fall technisch besehen um grenzüberschreitende Signale i.S.v. Art. 39 Abs. 1 NDG handelt. Es ist aber irreführend, zu suggerieren, dass damit irgendetwas darüber feststeht, wo sich die Kommunikationsteilnehmer aufhalten, man somit davon ausgehen könne, dass sich mindestens ein Kommunikationsteilnehmer im Ausland befindet, und dass die Beschränkung auf grenzüberschreitende Signale damit sicherstellen könne, dass die Kabelaufklärung auf den vom Gesetzgeber vorgesehenen Zweck beschränkt: Gemäss Botschaft zum NDG dient die Kabelaufklärung der Informationsbeschaffung über das Ausland. Die Kabelaufklärung ist ein Mittel der Auslandsaufklärung und bei der Kabelaufklärung sollen sich die Zielobjekte im Ausland befinden (Botschaft zum NDG, BBl 2014 2105, S. 2178). Wie sich aus den Ausführungen der Beschwerdeführenden ergibt,

ist dies aber damit, dass die Kabelaufklärung bei grenzüberschreitenden Signalen ansetzen muss, keineswegs gewährleistet.

10. Der Beschwerdegegner verweist hierzu ferner auf die Bestimmung von Art. 39 Abs. 2 NDG, wonach die beschafften Daten aus Signalen, bei denen sich sowohl der Sender als auch der Empfänger in der Schweiz befinden, soweit diese nicht bei der Erfassung ausgeschieden werden, zu vernichten sind, sobald erkannt wird, dass sie von solchen Signalen stammen (Ziff. 40 der Stellungnahme). Wie die Beschwerdeführenden mehrfach dargelegt haben, genügt dies jedoch nicht, insbesondere, weil bereits die initiale Erfassung einen Eingriff in die Grundrechte der an der Kommunikation beteiligten Personen bedeutet und weil diese Erkennung und Ausscheidung nicht zuverlässig funktionieren kann. Zudem bleibt – wie die Beschwerdeführenden bereits in ihrer Stellungnahme vom 15. März 2018 dargelegt haben – die Verwendung der erfassten Signale gemäss Art. 42 Abs. 3 NDG zulässig, sobald sich die IP des Senders und/oder des Empfängers im Ausland befinden: «Enthalten die Daten [nun nach der Rasterung] Informationen über Vorgänge im In- oder Ausland, die auf eine konkrete Bedrohung der inneren Sicherheit [...] hinweisen, so leitet der durchführende Dienst sie unverändert an den Nachrichtendienst weiter.» (Art. 42 Abs. 3 NDG). Unverändert bedeutet, dass die in Art. 42 Abs. 2 NDG vorgesehene Anonymisierung von Informationen über Per-sonen im Inland in diesem Fall nicht stattfindet.

11. Das Beispiel, das der Beschwerdegegner für die Erkennung von Schweiz-Schweiz-Kommunikation anführt, enthält technische Ungereimtheiten und geht im Ergebnis nicht auf: Der Beschwerdegegner schreibt, auch wenn anhand der über die Grenze versandten Datenpakete zum ausländischen Server natürlich nicht auf Anhieb erkannt werden könne, was das Endziel des darin enthaltenen Emails ist, so werde dies typischerweise möglich, sobald die Datenpakete zu einem Email zusammengesetzt seien. Diese müssten wiederum den Empfänger enthalten, damit der ausländische Server wisse, an welche IP-Adresse er sie weiterzusenden habe. Folglich könne selbst bei zwischengeschalteten Servern der Standort des Empfängers ermittelt werden. Der Beschwerdegegner vermengt hier zwei verschiedene Elemente, welche zur Anwendung gelangen, damit das Email vom Sender zum Empfänger gelangt: die Email-Adresse des Empfängers und die IP der empfangenden Stelle der Datenübermittlung. Empfangende Stelle ist beim Datenverkehr zwischen dem Absender des Emails und dessen Mailserver der Mailserver. Dementsprechend enthalten die versandten Datenpakete die IP des Mailservers. Sie enthalten jedoch nicht die IP des Empfängers selbst. Der Empfänger ist mittels seiner Email-Adresse bestimmt. Diese Email-Adresse wird zwar ersichtlich, wenn die versandten Datenpakete zu einem Email zusammengesetzt werden. Daraus ergibt sich aber nicht, wo der Empfänger das Email empfangen wird. Der Mailserver des Absenders muss (und kann) lediglich eruieren, an welchen Mailserver er das Email weiterschicken muss und welche IP dieser Mailserver hat. Die IP des Email-Empfängers ist dem Mailserver des

Absenders nicht bekannt und steht auch noch nicht fest. Die IP des Empfängers kommt dann ins Spiel, wenn dieser das Email auf sein Gerät herunterlädt, und hängt damit vom Standort des Geräts zum Zeitpunkt des Herunterladens ab. Denkbar ist beispielsweise, dass der Empfänger in Beirut wohnt, sich aber vorübergehend in Genf aufhält und dort das betreffende Email abruft (oder umgekehrt in Genf wohnt und das Email abruft, währenddem er sich in Beirut aufhält). Es ist damit unzutreffend, wenn der NDB meint, er könne aus den zusammengesetzten Paketen des Senders des Emails an dessen Server bzw. anhand der darin enthaltenen Email-Adresse des Empfängers eruieren, ob sich der Empfänger in der Schweiz oder im Ausland aufhält. Die Aussage des NDB, selbst bei zwischengeschaltetem Server könne der Standort des Empfängers ermittelt werden (Ziff. 41 der Stellungnahme), ist nicht haltbar.

12. Die Stellungnahme des Beschwerdegegners enthält weitere unzutreffende und irreführende Darlegungen in Bezug auf die Internetarchitektur. Der Beschwerdegegner schreibt, die Kommunikation von Personen in der Schweiz mit anderen Personen in der Schweiz bleibe im Regelfall in der Schweiz. Aus Effizienzgründen hätten die Internet-Provider kein Interesse daran, den Datenverkehr über das Ausland umzuleiten. Wer von Basel nach Zürich fahren wolle, nehme die direkte Strecke und nicht jene der deutschen Bahn über Schaffhausen (Ziff. 39 der Stellungnahme).

13. Die Funktionsweise des Internets lässt sich nicht sinnvoll und zutreffend mit einer Analogie zum Bahnverkehr umschreiben. Das Internet ist gänzlich anders organisiert als der Schienenverkehr. Zu berücksichtigen ist insbesondere, dass sich das Internet aus dem Zusammenspiel zahlreicher Provider ergibt, welche verschiedene Funktionen ausüben. Das Internet ist ein weltweites Netzwerk aus Netzwerken («Internet»), das eine paketvermittelte Kommunikation ermöglicht und auf mehreren Layern basiert. Es sei dazu auf die Ausführungen der Beschwerdeführenden in den vorangegangenen Rechtsschriften verwiesen, insbesondere auf Ziff. 28. ff. der Stellungnahme ans Bundesverwaltungsgericht vom 15. März 2018. Die Frage, welchen Weg Internetkommunikation in diesem Netzwerk aus Netzwerken nimmt, ist weit komplexer als die Frage, wo eine Person mit der Bahn durchreist.

14. Auch die Frage, wo die im weltweiten Netzwerk verwendeten Server stehen und inwieweit deren Standort lokalisiert werden kann, ist nicht so simpel, wie die Darlegungen des Beschwerdegegners vermuten lassen. Dieser Umstand lässt sich gerade an einem Beispiel zeigen, welches der Beschwerdegegner ins Feld führt: Der Beschwerdegegner legt anhand des Ergebnisses des Traceroute-Dienstes von Switch dar, dass sich ein Google-Server, an den eine Suchanfrage an Google aus der Schweiz geht, in der Schweiz befinde. Allerdings belegt er dies nicht etwa mittels einer Geolokalisation der IP, sondern mit dem Namen des Servers (zrh04s15-in-f3.1e100.net), welcher auf Zürich hindeutet («zrh» am Anfang des Namens). Eine Geolokalisation der dazugehörigen IP 172.217.168.67 (die

Ausführungen der Beschwerdeführenden zur Geolokalisation einer IP beruhen konkret auf den Ergebnissen von www.geolocation.com) ergibt allerdings als Resultat nicht Zürich, sondern Mountain View, California, USA – wenig überraschend, denn die IP gehört zu einem Adressbereich («Range») von Google, der von Geolokalisations-Diensten einem Google-Standort in Mountain View zugeordnet wird. Eine Google-Suche aus der Schweiz kann im Übrigen je nachdem auch bei einem anderen Google-Server landen.

15. Es ist im Übrigen auch nicht so, dass in der Schweiz tätige Internet-Provider ihre Infrastruktur und insbesondere ihre Server durchwegs in der Schweiz betreiben. So nutzte etwa UPC für seine Maildienste (highspeed.ch) lange Server in Österreich, welche inzwischen durch Server in den Niederlanden abgelöst wurden. Für UPC – inzwischen UPC Sunrise oder auch nur noch Sunrise – macht dies durchaus Sinn: Die betreffenden Server sind gemäss Geolokalisation Liberty Global zuzuordnen, dem Konzern, zu dem UPC Sunrise gehört. Das Beispiel zeigt die beschränkte Relevanz von Landesgrenzen für die Internet-Architektur und den Datenfluss im Internet.

16. Die Anbindung von in der Schweiz tätigen Internetprovidern an das weltweite Netz bzw. die Verbindungen der verschiedenen Provider untereinander sind eine vielschichtige Angelegenheit. So sind beispielsweise Swisscom, UPC Sunrise und Salt bedeutende Provider in der Schweiz, haben aber ihre Netzwerke sehr unterschiedlich aufgebaut bzw. sind unterschiedlich an das weltweite Netz angebunden. Der Datenverkehr zwischen Nutzern verschiedener Schweizer Provider kann über Verbindungen gehen, welche ausschliesslich durch die Schweiz gehen. Das muss aber nicht sein. Bei Datenverkehr zwischen UPC / Sunrise und anderen Schweizer Providern beispielsweise ist die Wahrscheinlichkeit hoch, dass die Verbindung über das Ausland geht; dasselbe gilt für Salt. Dies hat kurz gesagt vor allen Dingen damit zu tun, wie diese beiden Provider ihren Datenverkehr mit anderen Providern abwickeln, wobei bei UPC / Sunrise insbesondere auch die Einbindung in den Gesamtkonzern Liberty Global eine Rolle spielt.

17. Der Beschwerdegegner spricht an mehreren Stellen davon, dass ein Kabelaufklärungsauftrag für eine bestimmte Region genehmigt worden sei (so in Ziff. 39, Ziff. 43 u. Ziff. 58 der Stellungnahme). Dies erscheint ebenfalls als irreführend. Die Frage, auf welche Region ein Kabelaufklärungsauftrag zielt, wird dabei davon zu trennen sein, wie der Antrag für den Kabelaufklärungsauftrag formuliert ist. Art. 41 NDG sieht vor, dass die Kategorien von Suchbegriffen sowie die Betreiberinnen von leitungsgebundenen Netzen und der Anbieterinnen von Telekommunikationsdienstleistungen, deren Signale ausgeleitet werden sollen, angegeben werden müssen. Eine Eingrenzung auf eine bestimmte Region ist im Gesetz nicht vorgesehen, und es erscheint auch nicht als praktikabel, dass der Auftrag effektiv auf Daten einer bestimmten Region

eingegrenzt werden könnte. Bei Daten bzw. Informationen besteht aufgrund ihrer ubiquitären Natur das grundsätzliche Problem, dass sie eigentlich gar nicht lokalisierbar sein können.

18. Mehrmals, insbesondere in den Stellungnahmen vom 14. September 2021 und vom 12. Januar 2018, hat der Beschwerdegegner Ausführungen dazu gemacht, wie sich eruieren lasse, wo am ehesten Datenverkehr aus einem weiter entfernten Land wie Russland oder Syrien durchlaufe. Ergänzend zu unseren bisherigen Erläuterungen dazu sei darauf hingewiesen, dass gemäss Vernehmlassungsvorlage zum revidierten NDG neue Analysemöglichkeiten geschaffen werden sollen: Es wird vorgeschlagen, einen neuen Art. 42 Abs. 3bis NDG zu schaffen mit folgendem Wortlaut: «Der durchführende Dienst kann im Rahmen von bestehenden Aufträgen erfasste Signale und Daten analysieren, um technische Angaben über Datenströme zu gewinnen, die er nicht von den Betreiberinnen von leitungsgebundenen Netzen und den Anbieterinnen von Telekommunikationsdienstleistungen erhalten kann. Der NDB kann diese Erkenntnisse für die Formulierung der Anträge verwenden.» Im erläuternden Bericht wird dies wie folgt begründet: Beim Erlass des NDG sei man davon ausgegangen, dass die Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen – wie in Artikel 43 vorgesehen – in der Lage sind, hinreichende Auskünfte insbesondere über die von ihnen geführten internationalen Datenströme zu geben. In den ersten Anwendungsfällen der Kabelaufklärung habe sich aber gezeigt, dass das nur sehr bedingt zutreffe. Die Schweizer Betreiberinnen würden oft nur die Herkunfts- und Zielpunkte der Datenströme in den benachbarten Ländern und nicht deren weiterreichende Herkunft oder Endpunkte kennen. Wie diese Datenströme verliefen und welche Art von Kommunikationsdaten transportiert würden, sei einem stetigen, raschen Wandel unterworfen. Die internationalen Datenströme würden über hochdynamische Netzwerke geleitet, deren Routing sich rasch ändern und nicht langfristig vorausgesagt werden könne. Die Fernmeldedienstanbieterinnen würden ihre Datenflüsse permanent optimieren, sei es zugunsten einer besseren Übertragungsqualität, sei es aus wirtschaftlichen Überlegungen. Der durchführende Dienst solle deshalb neu die Rahmen von bestehenden Aufträgen erfassten Signale und Daten technisch analysieren dürfen, um ein möglichst aktuelles und realitätsgetreues Bild der bearbeiteten Datenströme, der damit transportierten Signale und der Herkunft und Destination der Kommunikationsdaten zu erhalten. Ebenfalls gelte es die technische Beschaffenheit der erfassten Signale zu ermitteln, weil dies einen direkten Einfluss auf die vom durchführenden Dienst zu deren Erfassung und Bearbeitung einzusetzenden technischen Mittel habe. Diese Art von Auswertung sei technischer Natur und nicht auf den Informationsgehalt der erfassten Daten bezogen. Solche technischen Informationen speichere der durchführenden Dienst ZEO der Schweizer Armee als Grundlagen für weitere Aufträge bei sich. Es gehe darum, zu erkennen, wo welche Arten von Datenströmen transportiert würden und

welche davon nachrichtendienstlich relevante Informationen enthalten könnten. Die dabei gewonnenen Erkenntnisse könne der durchführende Dienst mit dem Beschwerdegegner teilen, damit dieser die Formulierung der Kabelaufklärungsaufträge zielgerichteter vornehmen könne (d. h. Bezeichnung der zu überwachenden Datenströme in den Kabelaufklärungsaufträgen) (vgl. BBl 2022 1208). Die neu vorgeschlagene Bestimmung und die Begründung dieses Vorschlags im erläuternden Bericht zeigen eine ganz andere Einschätzung davon, wie zielgerichtet und effizient die Kabelaufklärung durchgeführt werden kann und wie gut es möglich ist, bei Kabelaufklärungsaufträgen gezielt grenzüberschreitende Datenleitungen auszuwählen, über welche Datenverkehr von und zu weiter entfernten Ländern vorwiegend läuft. Es offenbart sich hier, dass das VBS bzw. der Beschwerdegegner sich der von uns aufgezeigten Problematik durchaus bewusst ist.

19. Demgegenüber versucht der Beschwerdegegner in seiner Stellungnahme vom 18. August 2022 weiterhin, den Eindruck zu erwecken, die Kabelaufklärung könne so durchgeführt werden, dass ein konkreter Auftrag primär Daten einer bestimmten Region betrifft. Der Beschwerdegegner führt aus, die Kabelaufklärung beziehe sich auf Datenverkehr von und zu bestimmten, in den Anträgen an das Bundesverwaltungsgericht zu bezeichnenden und von diesem zu genehmigenden Regionen (z.B. Russland). Er müsse zudem ein bestimmtes Potenzial aufweisen, sicherheitspolitisch relevante Informationen zu beinhalten. Ferner müsse der Datenverkehr zu einem genehmigten und freigegebenen Kabelaufklärungsauftrag passen (Ziff. 43 der Stellungnahme). Wie von den Beschwerdeführenden dargelegt sehen die gesetzlichen Bestimmungen nicht vor, dass sich ein Antrag auf eine bestimmte Region beziehen und sich die im Rahmen des entsprechenden Kabelaufklärungsauftrag ausgeleiteten Daten auf solche von bzw. zu dieser bestimmten Region beschränken würden. Eine solche Beschränkung auf Daten mit Bezug zu einer bestimmten Region ist nicht nur nicht gesetztlich vorgesehen, sie liesse sich – selbst wenn dies im Antrag so aufgeführt würde – technisch auch gar nicht umsetzen. Es gibt keine grenzüberschreitenden Signale, welche z.B. lediglich oder überwiegend Daten von und nach Russland führen. Wie die Beschwerdeführenden dargelegt haben, ist nicht davon auszugehen, dass sich der grenzüberschreitende Datenverkehr mit Daten von und nach Russland primär auf einige wenige Verbindungen konzentriert, und es ist nicht ersichtlich, wie der Beschwerdegegner in der Lage sein soll, Verbindungen zu eruieren und für Kabelaufklärungsaufträge auszuwählen, über welche Daten von und nach Russland primär laufen. Die Ausführungen des NDB in der Stellungnahme vom 18. August 2022 vermögen an diesem Befund nichts zu ändern. Nachdem eine grenzüberschreitende Leitung, welche für einen Kabelaufklärungsauftrag in Frage kommt, nicht ausschliesslich oder überwiegend Daten zu bestimmten weiter entfernten Regionen führt, sondern regelmässig primär Daten von und nach anderen Ländern, läuft das Argument, die Regionen, um welche es gehe, würden nur einen

kleinen Teil des Internetverkehrs ausmachen (Ziff. 44 der Stellungnahme), ins Leere. Der Satz, der Datenverkehr müsse zu einem genehmigten und freigegebenen Kabelaufklärungsauftrag passen, stellt die Sachlage auf den Kopf. Der Datenverkehr, welcher über eine bestimmte Leitung läuft, ändert sich ja nicht und passt sich einem Kabelaufklärungsauftrag an, sobald ein solcher für diese Leitung genehmigt worden ist. Vielmehr ist es so – und liegt in der Natur eines solchen Massüberwachungsprogramms –, dass ein Kabelaufklärungsauftrag für bestimmte Leitungen und für bestimmte Suchbegriffe bzw. Kategorien von Suchbegriffen genehmigt wird. Hernach wird der betreffende Datenstrom komplett ausgeleitet und nach den vorgegebenen Begriffen durchsucht. Welche Daten effektiv durch diesen Datenstrom laufen, können der Beschwerdegegner und das Bundesverwaltungsgericht im vorangehenden Genehmigungsverfahren noch nicht wissen.

20. Der Äusserungen des Beschwerdegegners erscheinen auch hier als schwammig, nicht akkurat und schwer nachzuvollziehen. Sie vermögen zu der – wie eingangs dieser Stellungnahme dargelegt – notwendigen Untersuchung der Praxis der Kabelaufklärung nichts beizutragen. Nicht hilfreich ist dabei auch die Ambivalenz des Beschwerdegegners, einerseits sein Vorgehen bei der Kabelaufklärung erklären zu wollen, andererseits aber keine griffigen und stimmigen Beispiele dazu zu liefern und überdies geltend zu machen, er könne die Details zum Schutz der Aufklärung und der Provider nicht offen legen.

21. Was den Schutz der Provider betrifft (Ziff. 11 und 44 der Stellungnahme), ist dem Beschwerdegegner entgegenzuhalten, dass die dazu angeführte Bestimmungen in Art. 43 NDG lediglich Pflichten der Betreiberinnen von leitungsgebundenen Netzen und die Anbieterinnen von Telekommunikationsdienstleistungen umschreiben und dass sich die Pflicht zur Geheimhaltung gemäss Art. 43 Abs. 3 NDG wiederum lediglich auf die Betreiberinnen von leitungsgebundenen Netzen und die Anbieterinnen von Telekommunikationsdienstleistungen und auf die konkreten Aufträge, in welche sie involviert sind, beziehen. Der parteiöffentlichen Untersuchung der Praxis der Kabelaufklärung und den vom Beschwerdegegner hierbei zu erteilenden Auskünften stehen diese Bestimmung somit nicht entgegen. Die Untersuchung der Praxis der Kabelaufklärung erfordert wie dargelegt, dass sich das Bundesverwaltungsgericht und die Beschwerdeführenden ein zureichendes Bild über deren Funktionsweise machen können, was ohne substanzielle Erkenntnisse darüber, bei welcher Art von Providern (im weitesten Sinne) und bei was für Datenleitungen bzw. auf welchem Layer die Kabelaufklärung ansetzt und welche Arten von Daten ausgewertet werden, nicht möglich ist.

22. Ebenfalls der Berichtigung bedarf die Darstellung des Beschwerdegegners, wenn er es auf die Mailbox eines bestimmte Schweizer Benutzers oder auf seine Nutzung von Suchmaschinen abgesehen, so müsste er dafür eine andere, genehmigungspflichtige Massnahme einsetzen. Dies gelte auch,

wenn der Server im Ausland sei (Ziff. 50 Der Stellungnahme). Der Beschwerdegegner erweckt hier den Eindruck, der Auffassung zu sein, Funk- und Kabelaufklärung und genehmigungspflichtige Massnahmen würden sich insoweit gegenseitig ausschliessen, als Datenverkehr nicht mittels Funk- und Kabelaufklärung durchforstet werden dürfte, wenn damit die Kommunikation einer bestimmten Person aufgefunden werden soll, welche auch mittels genehmigungspflichtiger Massnahmen beschafft werden könnten. Dies geht aber nicht mit anderen Darlegungen des Beschwerdegegners zusammen, wie er bei der Funk- und Kabelaufklärung vorgehe, und entspricht auch nicht der Gesetzeslage: In der Stellungnahme vom 14. September 2021 referiert der Beschwerdegegner, potentiell betroffen von der Kabelaufklärung sei in erster Linie der Internet-Verkehr, der durch internationale Fernmeldekabel übertragen wird, z.B. Email-Verkehr, Internet-Suchanfragen oder Internettelefonie (Ziff. 30). In derselben Stellungnahme führt er aus, bei den verwendeten Suchbegriffen (Selektoren) handle es sich um spezifische Namen oder Identifikatoren (z.B. bekannte Telefonnummern, Email-Adressen) von verdächtigen Organisationen im Ausland (Mehrheit), von verdächtigen Einzelpersonen im Ausland (Minderheit) und weiteren konkreten verdächtigen Sachbezeichnungen (z.B. Modellbezeichnungen von Fernlenkwaffen, Kennungen von Nuklearmaterial, Bestellnummern bestimmter Dual-Use-Güter (Ziff. 64). Zwar sind Angaben über schweizerische natürliche oder juristische Personen als Suchbegriffe nicht zulässig (Art. 39 Abs. 3, letzer Satz, NDG). Eine Regelung, wonach die Kabelaufklärung dort, wo genehmigungspflichtige Massnahmen greifen, nicht zulässig ist, besteht nicht. Die beiden Arten von Massnahmen sind zudem derart unterschiedlich, dass sich die davon betroffenen Daten nicht trennscharf abgrenzen liessen: Es ist ohne Weiteres denkbar, dass Daten, welche sich mittels genehmigungspflichtiger Massnahmen beschaffen lassen, beispielsweise Email-Verkehr mittels einer Überwachung gemäss BÜPF, gleichzeitig zum Gegenstand einer Kabelaufklärungsmassnahme werden, wenn diese Daten über eine Datenleitung übertragen werden, welche von einem Kabelaufklärungsauftrag betroffen ist. Diese Daten werden in diesem Fall ausgeleitet, und es können sich in diesen Daten auch Übereinstimmungen mit den im Auftrag verwendeten Suchbegriffen ergeben, auch wenn die Email-Adresse, auf welche die genehmigungspflichtige Massnahme zielt, nicht zu den Suchbegriffen gehört.

23. Der Beschwerdegegner legt dar, die Schweiz verfüge über wichtige Telekomknotenpunkte und Transitstrecken, die sich für die Kabelaufklärung eignen würden. Dabei gehe es nicht nur um Internet-Verbindungen. Der Beschwerdegegner nennt dazu keine Details, welche nachvollziehbar machen, worauf er sich hier bezieht, sondern führt lediglich an, die Details seien dem Bundesverwaltungsgericht bekannt. Sodann schreibt er, Hinweise auf die Schweiz als Durchgangsstrecke für internationalen Fernmeldeverkehr würden sich aus öffentlichen Quellen wie beispielsweise Infrapedia ergeben. Er führt eine aus dieser Quelle

stammende Grafik an, welche zeigen würde, wie durch die Schweiz führende Telekommunikationsleitungen Italien und Teile von Südfrankreich mit dem Rest der Welt verbinden würden (Ziff. 52 der Stellungnahme). Daran hängt der Beschwerdeführer ein fiktives Beispiel von einem Waffenschieber in Moskau an, welcher mit seinem Mittelsmann in Italien kommunizieren will. In diesem Beispiel seien die Chancen gut, dass dieser Austausch über die im Bild dargestellte Alpentransit-Achse Frankfurt-Mailand durch die Schweiz laufe und somit überwacht werden könne (Ziff. 53 der Stellungnahme). Würden für eine solche Kommunikation Internetverbindungen benutzt, funktioniere die Lokalisierung der Sender und Empfänger über IP-Adressen sehr gut. Komme ein Datenstrom von einem Gerät in Russland und habe er als Ziel ein Gerät in Italien , sei die Wahrscheinlichkeit eines Senders oder Empfängers in der Schweiz trotz Beteiligung eines Schweizer Providers am Transport minimal (Ziff. 54 der Stellungnahme). Wo und wie genau der Beschwerdegegner auf solchen Knotenpunkten und Transitstrecken Kabelaufklärung betreibe und welche es sonst noch gibt, werde aus Gründen der Geheimhaltung nicht erläutert, aber das Prinzip werde klar (Ziff. 55 der Stellungnahme).

24. Effektiv vermengt der Beschwerdegegner hier so viele Ebenen und bleibt derart unkonkret, dass im Ergebnis gar nichts klar ist, und liefert damit ein weiteres Beispiel für Ausführungen, welche sich als nahezu wertlos erweisen. Der Beschwerdegegner schreibt einerseits, es gehe nicht nur um Internet-Verbindungen, und deutet an, dass sich solcher Nicht-Internet-Verkehr über wichtige Telekomknotenpunkte und Transitstrecken für Kabelaufklärung eigne. Anschliessend schreibt er von internationalem Fernverkehr. In seinem Beispiel ist dann von Kommunikation zwischen Moskau und Mailand die Rede, bei dem die Chancen gut stünden, dass sie über eine bestimmte Alpentransitachse Frankfurt-Mailand laufen würde. Dann macht er Ausführungen über die Lokalisierung von Sender und Empfänger solcher Kommunikation, wenn dafür Internetverbindungen benutzt würden.

25. Es bleibt unklar, was der Beschwerdegegner hier unter Internet-Verbindungen versteht und unter der Kommunikation, welche er nicht als Internet-Verbindungen erachtet, und ob der hier zu überwachende Verkehr jetzt nach seiner Anschauung Internetverkehr darstellt (was Ziff. 54 der Stellungnahme suggeriert) oder eben nicht (was Ziff. 52 der Stellungnahme nahe legt). Vor dem Hintergrund der technischen Gegebenheiten des heutigen Datenverkehrs und deren Topografie lässt sich den Ausführungen des Beschwerdegegners kein Sinn abgewinnen. Es ist unerfindlich, wie die Ausführungen des Beschwerdegegners auf Basis unserer Darlegungen zu Aufbau und Funktionsweise des Internets (vgl. insb. die Darlegungen in Ziff. 28. ff. der Stellungnahme der Beschwerdegegner ans Bundesverwaltungsgericht vom 15. März 2018, welche ihrerseits auf dem massgebenen OSI-Modell [https://de.wikipedia.org/wiki/OSI-Modell] beruhen) zu verstehen wären.

Was der Beschwerdegegner mit den erwähnten wichtigen Telekomknotenpunkten und Transitstrecken meint, ist nicht greifbar, und ebenso wenig, worauf er sich beziehen könnte, wenn er ausführt, es gehe nicht nur um Internet-Verbindungen, zumal über Telekommunikationsnetze mit hohen Datenübertragungsraten, welche auf Glasfaser basieren, kurz gesagt eine Vielzahl verschiedener Daten laufen kann (das gilt gerade auch für jene Datenleitungen, welche man als Transitstrecken bezeichnen könnte). Ohne dass der Beschwerdegegner deutlich macht, was er unter Knotenpunkten und Transitstrecken versteht und auf welche Layer und welche Protokolle er sich bezieht, bleiben seine Ausführungen nebulös.

26. Im Zusammenhang mit den vorgeblichen Zielregionen, auf welche die ausgeleiteten Verbindungsstrecken ausgerichtet seien, bringt der Beschwerdegegner vor, in diesen Zielregionen sei es um Verschlüsselung oft anders bestellt als in der Schweiz. Die dortigen Regimes wollten auf sämtliche Kommunikation zugreifen können und würden in solchen Fällen eine sichere Verschlüsselung kurzerhand verbieten. Dazu führt der Beschwerdegegner das Beispiel der Verurteilung von Telegram 2018 in Russland an, auch gegen Threema seien die russischen Behörden wegen seiner Verschlüsselung vorgegangen (Ziff. 59 der Stellungnahme). Der Beschwerdegegner unterschlägt, dass das Vorgehen der russischen Behörde wirkungslos blieb. Die Bemühungen, Telegram zu blockieren, wurden schliesslich aufgegeben (vgl. https://www.heise.de/news/Russland-gibt-Blockadeversuche-gegen-Telegram-auf-4788894.html).

27. Weiter führt der Beschwerdegegner aus, andere Regionen könnten aufgrund des Alters ihrer IT-Infrastruktur nicht sicher verschlüsseln. Manche Mail-Server in CIS-Ländern würden beispielsweise noch keine moderne TLS-Verschlüsselung unterstützen. Bei einer Kommunikation mit einem Mailserver in Italien sei die Übermittlung gar nicht oder nur ungenügend geschützt. Tue dies ein normaler Schweizer Mail-Server, verhindere TLS 1.2 oder 1.3 den Zugriff auf seine E-Mails im Klartext (Ziff. 60 der Stellungnahme). Die vom Beschwerdegegner behauptete Korrelation zwischen bestimmten Ländern bzw. Ländergruppen und dem allgemeinen Stand der Verschlüsselung von Kommunikation in den entsprechenden Ländern erscheint nicht als haltbar. Inbesondere ist fraglich, was hier mit der IT-Infrastruktur der bestehenden Region gemeint sein könnte und in wie weit diese den Möglichkeiten entgegenstehen soll, in der betreffenden Region verschlüsselt kommunizieren und insbesondere Mails-Server betreiben zu können, welche TLS 1.2 oder 1.3 beherrschen.

28. Auf die Erwiderungen des Beschwerdegegners gegen die Darlegungen der Beschwerdeführenden zur Tätigkeit der Aufsichtsorgane und zur gerichtlichen Überprüfung gehen die Beschwerdeführenden in der vorliegenden Stellungnahme nicht in allen Details ein. Darauf wird im Verlauf des weiteren Instruktionsverfahrens zurückzukommen sein,

mutmasslich, nachdem die Stellungnahmen vorliegen, welche das Bundesverwaltungsgericht mit Verfügung vom 9. September 2022 angefordert hat. An dieser Stelle kann festgehalten werden, dass der Beschwerdegegner die Ausführungen der Beschwerdeführenden entstellt und sinnwidrig wiedergibt. Nicht stehen lassen können die Beschwerdeführenden die Unterstellung, sie hätten dem Bundesverwaltungsgericht schlampige Arbeit vorgeworfen. Die Beschwerdeführenden haben vielmehr thematisiert, wie effektiv eine gerichtliche Überprüfung von geheimdienstlichen Überwachungsmassnahmen sein kann, und haben auf Begrenzungen hingewiesen, welche sich aus den gesetzlichen Voraussetzungen der Massnahmen und dem dem Gericht obliegenden Prüfungsprogramm ergeben. Zur gerichtlichen Genehmigung einzelner Funk- und Kabelaufklärungsaufträge ist überdies zu bemerken, dass sich diese mit einzelnen Aufträgen befasst und nicht dazu gedacht ist, die effektiven Überprüfung des Systems der Funk- und Kabelaufklärung leisten, welche das Bundesverwaltungsgericht gemäss Rückweisungsentscheid des Bundesgerichts und gemäss Rechtsprechung des EGMR vorzunehmen hat, und dass die gerichtliche Genehmigung einzelner Funk- und Kabelaufklärungsaufträge eine solche Überprüfung auch nicht leisten könnte.

Mit freundlichen Grüssen

Viktor Györffy

Im Doppel