Peyrot, Schlegel & Györffy
Rechtsanwälte

Zürich, 15. März 2018

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-6143/2017

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 16. Januar 2018 und reiche Ihnen innert der entgegenkommenderweise erstreckten Frist zur Vernehmlassung des Beschwerdegegners folgende **Stellungnahme** ein:

1. Der Beschwerdegegner vertritt die Auffassung, auf das Rechtsschutzansuchen der BeschwerdeführerInnen sei nicht einzutreten gewesen. Er argumentiert, die BeschwerdeführerInnen hätten keinen «Sondernachteil» dargelegt, und ein solcher ergebe sich auch nicht aus den Akten. Er wirft den BeschwerdeführerInnen vor, sie hätten davon abgesehen, ein datenschutzrechtliches Einsichtsgesuch zu stellen. Die BeschwerdeführerInnen seien deshalb nicht mehr als jedermann von der Funk- und Kabelaufklärung betroffen.

2. Die Argumentation des Beschwerdegegners ist nicht ohne Weiteres nachvollziehbar, zumal sich darin weder die relevanten rechtlichen Grundsätze noch die Vorbringen der BeschwerdeführerInnen widerspiegeln. Massgeblich ist, ob den BeschwerdeführerInnen gemäss Praxis der Strassburger Organe die Möglichkeit gegeben werden muss, die Grundrechtskonformität mit der Funk- und Kabelaufklärung verbundenen Überwachung mit einem Rechtsmittel überprüfen zu lassen. Soweit die Beschwerdelegitimation gemäss der Praxis der Strassburger Organe zu bejahen ist, sind die innerstaatlichen Organe verpflichtet, auf ein diesbezügliches Ersuchen einzutreten.

3. Bei geheimen Überwachungsmassnahmen und verstärkt noch bei Massenüberwachungsprogrammen besteht die Problematik, dass die Betroffenen regelmässig nicht wissen, in wie weit sie konkret davon betroffen sind. In einer weit zurückreichenden Praxis lassen die Strassburger Organe deshalb zu, dass eine Person unter gewissen Voraussetzungen behaupten kann, durch die blosse Existenz geheimer Massnahmen oder einer Gesetzgebung, die solche Massnahmen erlaubt, Opfer einer Verletzung zu sein, ohne dass sie vorbringen muss, dass sie solchen Massnahmen tatsächlich ausgesetzt war. Der EGMR hat erkannt, dass Art. 8 EMRK sonst Gefahr läuft, faktisch ausgehebelt zu werden. Denn wer nie erfährt, dass er überwacht worden ist, kann sich auch nicht dagegen wehren (vgl. Szabó and Vissy v. Hungary [37138/14], EGMR, 12. Januar 2016, § 32 ff.; Liberty and Others v. The United Kingdom [58243/00], EGMR 12. Juli 2008, § 56 f.; Weber and Saravia v. Germany [54934/00], EGMR, 29. Juni 2006; Klass and Other v. Germany [5029/71], EGMR [Plenum], 6. September 1978, § 33 ff. [EuGRZ: www.eugrz.info/pdf/EGMR31.pdf], je m.w.H.; Kennedy v. The United Kingdom [26839/05], EGMR, 18. Mai 2010, § 124; Roman Zakharov v. Russia [47143/06], EGMR [Plenum], 4. Dezember 2015, § 170 ff.).

4. In ihrer aktuellen Praxis prüfen die Strassburger Organe, ob die beschwerdeführende Person in den Anwendungsbereich des entsprechenden Gesetzes fällt und von Überwachung betroffen sein kann, weil sie zu der Personengruppe gehört, auf welche die Gesetzgebung abzielt oder weil überhaupt alle Nutzer von Kommunikationsdiensten betroffen sind. Sodann stellt der Gerichtshof darauf ab, ob auf nationaler Ebene wirksame Rechtsbehelfe vorhanden sind. Wo es keine effektiven Rechtsbehelfe gibt, mit welchen die Rechtmässigkeit der Überwachung überprüft werden kann, ist der Verdacht auf Missbrauch nicht abwegig. Gleichzeitig ist in dieser Situation die Gefahr einer Überwachung geeignet, die freie Kommunikation via Post- und Fernmeldedienste zu beeinträchtigen, so dass für alle Nutzer solcher Dienste ein Eingriff in das Recht auf Privatsphäre nach Art. 8 EMRK vorliegt. Es besteht daher erhöhter Bedarf für eine genaue Prüfung durch den Gerichtshof. Die beschwerdeführende Person muss also nicht beweisen können, dass sie von einer Massnahme konkret betroffen ist. Wo hingegen effektive Rechtsbehelfe vorliegen, ist eine generelle Angst vor Missbrauch schwieriger zu rechtfertigen. Daher muss die beschwerdeführende Person darlegen, warum aufgrund ihrer persönlichen Situation die Gefahr besteht, dass sie von geheimen Überwachungsmassnahmen betroffen ist (vgl. Kennedy v. The United Kingdom [26839/05], EGMR, 18. Mai 2010, § 124; Roman Zakharov v. Russia [47143/06], EGMR [Plenum], 4. Dezember 2015, § 170 ff.).

5. Bei der Funk- und Kabelaufklärung werden bestimmte Kommunikationsströme gesamthaft gescannt, aus den gescannten Daten werden computergestützt Hits generiert. Ob hinter allfälligen Hits effektiv nachrichtendienstlich relevante Vorgänge stehen, kann der

Beschwerdegegner regelmässig nicht wissen, sondern höchstens vermuten. Es handelt sich hier um ein Massenüberwachungskonzept, in das bewusst Kommunikation von sehr vielen unbescholtenen Personen einbezogen wird und das alle treffen kann, welche elektronische Kommunikationskanäle nutzen. Die Überwachung beginnt dabei mit dem Scannen und automatisierten Analysieren der Kommunikationsströme und setzt sich gegebenenfalls durch eine weitere Bearbeitung und Speicherung fort. Auch die dem NDB zudienende Tätigkeit des ZEO ist nachrichtendienstliche Tätigkeit im Sinne des NDG. Ungeachtet der konkreten Organisation und Arbeitsteilung ist die Tätigkeit des ZEO letztlich dem NDB zuzurechnen. Von daher und vor dem Hintergrund der Praxis der Strassburger Organe erscheint der Ansatz des Beschwerdegegners, wie er die Legimation abhandelt, nicht als zielführend. Der vom Beschwerdegegner gewählte Ansatz des «Sondernachteils» verträgt sich schlecht mit dem Konzept der Massenüberwachung.

6. Der Beschwerdegegner macht in seiner Vernehmlassung Aussagen dazu, welche Kommunikation von der Funk- und Kabelaufklärung erfasst wird. Diese Ausführungen sind aufschlussreich, aber gleichzeitig irreführend. Die Funk- und Kabelaufklärung setzt ja an bestimmten Datenströmen an, indem etwa eine bestimmte Glasfaserleitung gescannt wird. Wie nachstehend erläutert wird (Ziff. 27. ff.), sind aufgrund der Netzwerkarchitektur und der Art und Weise, wie Daten in Netzwerken transportiert werden, nur begrenzt Aussagen darüber möglich, welche Daten über bestimmte Datenströme fliessen und welche nicht.

7. Um es am Bild der Nadel im Heuhaufen zu verdeutlichen: Überwacht wird nicht ein eingegrenzter Heuhaufen, sondern der gesamte Datenfluss, welcher stetig über einen bestimmten Kanal läuft. Welche Daten über diesen Kanal laufen, ist aufgrund Funktionsweise der netzwerkgebundenen Kommunikation letztlich nicht eindeutig bestimmbar. Welches die Nadeln im Haufen sind, weiss der NDB nicht, er kann lediglich mittels computergestützter Analysen zu interpretieren versuchen, was Heu und was Nadel ist. Die Beschwerdegegnerin kann unter diesen Umständen nicht ernsthaft behaupten, die BeschwerdeführerInnen seien nicht von der Funk- und Kabelaufklärung tangiert.

8. Vielmehr muss jede Person damit rechnen, dass ihre elektronische Kommunikation über einen Kanal läuft, welcher von der Funk- und Kabelaufklärung erfasst wird. Diese Überwachung betrifft sämtliche Nutzer elektronischer Kommunikation, da sie als Massenüberwachung konzipiert ist und da bei der Vielfalt der Kommunikationswege im Netz und der Vielfalt der genutzten Kommunikationsdienste jede Person damit rechnen muss, dass Kommunikation von ihr einen Kommunikationskanal durchläuft, welcher mit Funk- und Kabelaufklärung gescannt wird.

9. Wie bereits in der Beschwerde dargelegt bedeutet ein Hit noch lange nicht, dass damit Kommunikation aufgespürt worden ist, welche sich auf nachrichtendienstlich relevante Vorgänge bezieht. Es ist Teil des Konzepts und unvermeidlich, dass auch die Kommunikation unbescholtener Personen gescannt wird und allenfalls Hits generiert. Gleichzeitig wird es sehr oft kaum möglich sein, zu erkennen, dass es sich ungeachtet eines Hits um unbescholtene Personen handelt. So können Hits zu zweifelhaften Vermutungen führen, auf deren Basis Personen fälschlicherweise in den Fokus des Nachrichtendienstes geraten. Auch aufgrund dieser der Funk- und Kabelaufklärung immanenten Unschärfe ist zu konstatieren, dass mit diesem Überwachungsmittel jede Person zum Ziel nachrichtendienstlicher Tätigkeit werden kann.

10. Ein Beispiel dafür, wie eine Person rein aufgrund der von ihr verwendeten Wörter fälschlicherweise in den Verdacht geraten kann, einer terroristischen Vereinigung anzugehören, ist der Fall des Berliner Stadtsoziologen Andrej Holm. Er wurde wegen Verdachts auf Mitgliedschaft in einer terroristischen Vereinigung festgenommen und war über längere Zeit einer umfassenden Überwachung ausgesetzt. Grund dafür waren vor allen Dingen Mutmassungen, er könnte der Autor von Texten einer als terroristisch eingestuften Gruppierung sein. Diese Mutmassungen basierten auf dem blossen Umstand, dass Andrej Holm als Stadtsoziologe bei gentrifizierungskritischen Äusserungen in wissenschaftlichen Publikationen dieselbe Terminologie verwendete wie die betreffende Gruppierung in ihren Verlautbarungen. Obschon es über diese terminologischen Übereinstimmungen hinaus nichts Greifbares gab, war der einmal gehegte Verdacht über längere Zeit nicht wegzubringen. Das Verfahren wurde im September 2006 eingeleitet und am 5. Juli 2010 mangels hinreichendem Tatverdacht eingestellt. Die Strafverfolgungsbehörden hielten trotz der anhaltend dürftigen Indizienlage jahrelang an ihrer ursprünglichen Interpretation der Indizien fest (vgl. https://de.wikipedia.org/wiki/Andrej_Holm).

11. Dieselbe Logik, welche Andrej Holm den Verdacht eintrug, er sei mutmasslicher Terrorist, kann dazu führen, dass eine unbescholtene Person rein aufgrund der Wortwahl in ihrer Kommunikation oder vergleichbarer Indizien Hits in der Funk- und Kabelaufklärung generiert, dass dies zur falschen Annahme führt, die Person gehe nachrichtendienstlich relevanten Tätigkeiten nach, was die Erfassung und Bearbeitung von Daten dieser Person durch den NDB zur Folge hat, und dass diese falsche Annahme über lange Zeit nicht mehr wegzubringen ist.

12. Im Unterschied zu dem gegen Andrej Holm geführten Strafverfahren wird eine von der Funk- und Kabelaufklärung betroffene Person in aller Regel nicht von den vom Nachrichtendienst gehegten Verdächtigungen erfahren und wird damit auch keine Gelegenheit erhalten, sie richtigzustellen. Es bestehen keine strafprozessualen Garantien, und es existiert kein Prozedere wie im Strafprozess, wo ein einmal eröffnetes Verfahren innert

nützlicher Frist auf den Punkt gebracht und formell abgeschlossen werden muss.

13. Je stärker beim Scannen und Auswerten der Daten auf Algorithmen, Künstliche Intelligenz (KI) und Machine Learning abgestützt wird, desto weniger wird für die Personen, welche die Daten auswerten und über deren weitere Verwendung entscheiden sollen, nachvollziehbar sein, was genau zu Hits führt und was deren Relevanz ist. Solche Technologien werden nicht zuletzt eingesetzt, um Zusammenhänge herauszuarbeiten, welche sonst nicht gesehen werden. Dabei geht es u.a. um die Auswertung von Mustern, welche sich in grossen Datenmengen feststellen lassen, um die Kombination verschiedener Merkmale über eine grosse Datenmenge hinweg und darum, dass der Computer bei der Auswertung von Daten laufend dazulernt. Bei KI und Machine Learning arbeitet der Computer nicht einfach Daten nach einer vorgegebenen Programmierung ab, sondern modifiziert den Datenbearbeitungsprozess selbständig. Auf diese Weise koppelt sich die Datenverarbeitung mehr und mehr von den ursprünglichen Vorgaben ab, und genau darum geht u.a. auch beim Einsatz von KI: Auf diese Weise sollen durch die computergestützte Datenverarbeitung Möglichkeiten erschlossen werden, welche herkömmliche analytische Ansätze übersteigen. Je mehr aber die Analyse von KI geprägt ist, desto weniger wird dessen Ergebnis nachvollziehbar und überprüfbar (es sei dazu im Detail auf die Beschwerdeschrift verwiesen, insb. Ziff. II. B. 28. und Ziff. II. D. 9. ff.). Bei der Funk- und Kabelaufklärung führt dies u.a. dazu, dass die vom Computer vorgenommene Analyse der gescannten Daten durch neurolinguistische Datenverarbeitung unter Verwendung von Konzepten von Big-Data, KI und Machine-Learning mit fortschreitender Analyse mehr und mehr über die vorgegebenen Suchbegriffe hinausgehen wird. Der NDB kann sich so auch vom Computer neue Suchbegriffe liefern lassen und die Funk- und Kabelaufklärung im Vertrauen darauf, dass der Computer «wissen» wird, weshalb die zusätzlichen Suchbegriffe sinnvoll erscheinen, dem entsprechend ausdehnen.

    Für eine fundierte Klärung der diesbezüglichen Zusammenhänge, insbesondere der mit der Funk- und Kabelaufklärung verbundenen Möglichkeiten der Datenauswertung, wird **beantragt**, ein Sachverständigengutachten bei einem Computerlinguisten oder einer vergleichbaren Fachperson einzuholen.

14. Innerstaatliche Rechtsbehelfe, mit denen die Überwachung unbescholtener Personen zureichend eingedämmt werden könnten, bestehen nicht. Die Überwachung beginnt beim automatisierten Scannen der Datenströme. Hier ist gerade nicht das Ziel, nur verdächtige Kommunikation bzw. nur Kommunikation verdächtiger Personen zu erfassen, sondern möglichst viel Kommunikation vieler Personen, welche dann gesamthaft gescannt wird. Diese computergestützte Überwachung zielt bewusst auch auf die Kommunikation völlig unbescholtener Personen. Bereits insoweit fehlt es

an wirksamen Rechtsbehelfen, welche sicherstellen könnten, dass die Kommunikation unbescholtener Personen nicht überwacht wird.

15. Kabelaufklärungsaufträge werden gestützt auf einen Entscheid des Bundesverwaltungsgerichts geschaltet, mit dem die betroffenen Kommunikationskanäle und die zu verwendenden Kategorien von Suchbegriffen festgelegt werden. Dieser Entscheid spezifiziert die konkrete Überwachung. Er grenzt sie aber insoweit nicht ein, als danach die gesamte Kommunikation gescannt und damit überwacht wird, welche über den entsprechenden Kanal läuft. Der Entscheid ändert m.a.W. nichts daran, dass die Funk- und Kabelaufklärung den Charakter einer Massenüberwachung hat. Durch die Festlegung der Kategorien von Suchbegriffen wird die Überwachung thematisch ein Stück weit eingegrenzt. Die konkreten Suchbegriffe bzw. die zu verwendenden Algorithmen werden aber nicht vom Bundesverwaltungsgericht festgelegt, sondern vom NDB. Die Suche kann so laufend modifiziert werden, auch unter Verwendung von Künstlicher Intelligenz und Machine Learning, was die begrenzende Funktion des Genehmigungsentscheids des Bundesverwaltungsgerichts stark aufweicht.

16. Es ist im Übrigen darauf hinzuweisen, dass für die Funkaufklärung, deren Grundrechtskonformität ja wie dargelegt bereits vor Jahren von der GPDel in Frage gestellt worden ist, keine richterliche Genehmigung vorgesehen ist.

17. Ein Hit bedeutet wie gesagt nicht unbedingt, dass einschlägige Kommunikation vorliegt. Der Hit wird vom Computer aus einer Massenüberwachung generiert. Der Hintergrund der Kommunikation ist damit nicht ohne Weiteres klar. Der NDB und der ZEO können die betreffende Kommunikation lediglich interpretieren. Wir die Kommunikation für relevant erachtet, so ist dies nur das Ergebnis einer entsprechenden Interpretation. Diese kann auch falsch sein. Der Funk- und Kabelaufklärung ist damit immanent, dass Daten, die daraus gewonnen und in den einschlägigen Systemen gespeichert und bearbeitet werden, auch Kommunikation von unbescholtenen Personen enthalten. Der NDB vermag mit seiner Analyse nicht zu gewährleisten, dass die Daten unbescholtener Personen ausgeschieden werden. Ebenso wenig kann dies durch nachgeordnete interne oder externe Kontrollen der Tätigkeit des NDB gewährleistet werden. Für eine solche Gewährleistung fehlt den involvierten Personen regelmässig nur schon das notwendige Hintergrundwissen. Es ist dem Konzept immanent, dass auch Hits verwendet werden, bei welchen aufgrund von Fehlinterpretationen und mangels weiterem Hintergrundwissen nicht erkannt wird, dass es sich hier um Kommunikation einer unbescholtenen Person handelt. Auch wird sich die Datenerfassung und -bearbeitung nicht gesamthaft, sondern nur im Ansatz und stichprobenweise überprüfen lassen. Die vorgesehenen Aufsichts- und Kontrollmechanismen genügen jedenfalls, wie bereits in der Beschwerdeschrift dargelegt, nicht.

Nachdem der Beschwerdegegner Behauptungen über die Wirksamkeit der Aufsicht und Kontrolle aufstellt, die klar unzutreffend erscheinen bzw. die Problematik vernebeln, und nachdem nicht a priori feststeht, wie genau und in welchem Umfang die Funk- und Kabelaufklärung von den Aufsichts- und Kontrollorganen überprüft wird, wird **beantragt**, folgende vom Beschwerdegegner in diesem Zusammenhang erwähnten Organe und Gremien zur diesbezüglichen Aufsicht und Kontrolle in einer Anhörung zu befragen:

- die Qualitätssicherungsstelle NDB;
- die GPDel;
- die Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND) sowie
- die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung.

18. Die Person, deren Daten gescannt und allenfalls gespeichert und bearbeitet werden, erfährt in aller Regel nichts von der Datenbearbeitung und kann sich selbst nicht wirksam dagegen wehren. Datenbearbeitung liegt vor, sobald Kommunikation durch einen von der Funk- und Kabelaufklärung erfasste Datenleitung läuft und automatisch gescannt wird. Über diese Datenbearbeitung werden die betroffenen Personen per se nie orientiert. Ergibt sich ein Hit, so werden die Daten von Mitarbeitern des ZEO und allenfalls des NDB gesichtet, allenfalls, ohne in einem Informationssystem gespeichert zu werden. Über diesen weiteren Schritt der Datenbearbeitung per se wird von Amtes wegen ebenfalls niemand orientiert. Werden die Daten, welche sich aus dem Hit ergeben, in einem Informationssystem gespeichert und weiter bearbeitet, so wird die betroffene Person davon in den meisten Fällen ebenfalls nichts erfahren. Die betroffene Person verfügt lediglich über das Auskunftsrecht im Rahmen von Art. 63 NDG, welches aber nicht die gesamte beschriebene Datenbearbeitung erfassen kann, sondern lediglich die in einem Informationssystem abgespeicherten Daten. Da die Überwachung bzw. die damit verbundene Speicherung und Verarbeitung der Daten heimlich erfolgen, wird die betroffene Person regelmässig keine Veranlassung sehen, vom Auskunftsrecht Gebrauch zu machen. Eine obligatorische Mitteilung, wie man sie etwa im Strafprozess kennt und mit Einschränkungen auch bei genehmigungspflichtigen Beschaffungsmassnahmen, ist im Zusammenhang mit Daten aus der Funk- und Kabelaufklärung nicht vorgesehen.

19. Zudem besteht noch die Problematik, dass die von der Funk- und Kabelaufklärung erfassten Daten, welche regelmässig fragmentarischen Charakter haben, vom NDB möglicherweise gar nicht der Person zugeordnet werden können, welche es betrifft. Dies gilt nicht nur für das automatisierte Scannen der Daten und die unmittelbar daran anschliessende Datenbearbeitung, sondern auch, soweit Daten in einem Informationssystem gespeichert werden. In einigen Fällen wird die

Zuordnung zu einer Person aufgrund der vorhandenen Daten – solche, die aus der Funk- und Kabelaufklärung stammen und allenfalls weitere, mit denen diese kombiniert werden – akkurat möglich sein, in anderen nicht. Ein allenfalls gestelltes Auskunftsersuchen kann insoweit ins Leere laufen.

20. Insgesamt bestehen damit keine effektiven Rechtsbehelfe, mit welchen sichergestellt werden könnte, dass nur grundrechtskonforme Überwachung und Datenbearbeitung stattfindet. Auch der Schutz vor einer Weitergabe von Daten an andere Stellen und Behörden in In- und Ausland ist ungenügend. Es sei dazu auch auf die entsprechenden Darlegungen in der Beschwerde verwiesen. Die Beschwerdeführer haben aufgezeigt, dass die bestehenden Kontrollmechanismen nicht zu genügen vermögen. Sie haben auch darauf hingewiesen, dass der journalistische Quellenschutz und die Wahrung der Berufsgeheimnisse bei der Funk- und Kabelaufklärung nicht gewährleistet sind. Die Gewährleistung dieser Garantien ist im NDG nicht vorgesehen. Selbst dann, wenn der NDB und die involvierten Kontroll- und Aufsichtsinstanzen in der Praxis versuchen würden, etwas zum Schutz dieser Garantien zu tun, könnte dem kein Erfolg beschieden sein. Kommunikation, welche über ein von der Funk- und Kabelaufklärung betroffenes Signal läuft, wird unterschiedslos erfasst, auch dann, wenn die Kommunikation dem journalistischen Quellenschutz oder einem Berufsgeheimnis unterliegt.

21. Soweit der Beschwerdegegner in seiner Vernehmlassung darauf verweist, dass die Funk- und Kabelaufklärung den gesetzlich definierten Zwecken dienen muss und auf die bestehenden Abläufe und Kontrollen hinweist, mit denen die Datenbeschaffung auf relevante Information begrenzt werden soll, erscheint dies gelinde gesagt als blauäugig. Aufgrund der Natur der nachrichtendienstlichen Massenüberwachung vermag dies effektiv keine Grundrechtskonformität zu gewährleisten. Auch die Überlegung, durch die sorgfältige und gezielte Auswahl der Kategorien von Suchbegriffen und der zu verpflichtenden Fernmeldedienstanbieter werde sichergestellt, dass von Beginn weg nur Daten zur weiteren Verarbeitung gelangen, welche mit hoher Wahrscheinlichkeit auftragsrelevante Informationen enthalten, andernfalls wäre davon auszugehen, dass das Bundesverwaltungsgericht den Antrag nicht genehmigen würde, geht fehl. Mit der Genehmigung von Kategorien von Suchbegriffen und der Auswahl der zu scannenden Leitungen kann die Überwachung wie dargelegt nicht wirksam auf relevante Kommunikation eingegrenzt werden.

22. Auch wenn der Beschwerdegegner immer wieder betont, dass es um die Erfassung von relevanten Informationen geht und ausführt, welche Daten ausgeschieden würden, ist doch zu konstatieren, dass kein Prozedere besteht, welches die Grundrechtskonformität der Überwachung und Datenbearbeitung zu gewährleisten vermöchte. Die Funk- und Kabelaufklärung stellt wie gesagt eine Massenüberwachung dar, mit welcher Daten verarbeitet werden, bei denen regelmässig nicht feststeht,

was für eine Bewandtnis es mit ihnen hat. Es fehlt den mit der Funk- und Kabelaufklärung betrauten Organen damit regelmässig bereits das Wissen, um beurteilen zu können, ob die an der Kommunikation beteiligten Personen nachrichtendienstlich relevanten Tätigkeiten nachgehen. Zudem schaffen die vom Beschwerdegegner dargelegten Mechanismen keine wirksamen Garantien für die Nichterfassung oder Aussonderung der Kommunikation unbescholtener Personen.

23. Hier verschränkt sich die oft dürftige, immer interpretationsbedürftige Sachlage in Bezug auf die Relevanz der Kommunikation mit mangelhaften Regelungen zur Begrenzung der Erfassung und Verarbeitung von Daten. Ein Beispiel dafür liefert der Beschwerdegegner selbst mit diesen Ausführungen:

> *«Die auf den ausgewählten Fasern enthaltenen Daten werden nach den im Kabelaufklärungsauftrag definierten Kategorien von Suchbegriffen (beispielsweise Telefonnummern, IP Adressen, Schlüsselwörter) durchsucht und durch einen Analysten des ZEO ausgewertet. Dabei wird durch den Analysten noch einmal sichergestellt, dass die an den NDB weitergeleiteten Informationen auftragskonform sind oder direkte Hinweise auf eine Gefährdung der inneren oder äusseren Sicherheit enthalten und keine rein schweizerische Kommunikation enthalten (entsprechende Daten müssen vom ZEO vernichtet werden).»*

24. Zwar wird hier die Gefährdung der inneren oder äusseren Sicherheit erwähnt, es soll aber genügen, wenn der Analyst des ZEO sicherstellt, dass die Informationen *«auftragskonform»* sind – ein sehr vager Ansatz, den der Analyst wohl getrost als erfüllt erachten kann, wenn er die Information im Zweifelsfall einfach einmal weiterleitet. Er wird ohnehin aufgrund der ihm vorliegenden Informationen nicht in der Lage sein, die Grundrechtskonformität der Datenerfassung zu beurteilen, und auch ob es sich um rein schweizerische Kommunikation handelt, wird er oftmals nicht erkennen können. Eine Gewährleistung der Rechtskonformität der Datenbearbeitung wird der Analyst jedenfalls nicht liefern können. Auch die im Zusammenhang mit der Funk- und Kabelaufklärung bestehenden Kontrollmöglichkeiten vermögen die Rechtskonformität nicht zu gewährleisten bzw. bei Daten, welche fälschlicherweise erfasst und in den Datenbestand der einschlägigen Informationssysteme eingegangen sind, wiederherzustellen. Die Kontrollorgane wissen ja gar nicht, dass der Eintrag da ist, es sei denn, sie stossen bei einer Stichprobe darauf, und sie werden die Grundrechtskonformität der Überwachung in vielen Fällen auch nicht effektiv beurteilen können. Wie an anderer Stelle dargelegt ist insgesamt auch nicht sichergestellt, dass rein schweizerische Kommunikation nicht gespeichert und verarbeitet wird.

25. Die Legimation ist den BeschwerdeführerInnen somit bereits deshalb zuzugestehen, weil von der Funk- und Kabelaufklärung letztlich alle NutzerInnen von Kommunikationsdiensten betroffen sind, also auch die BeschwerdeführerInnen, welche Kommunikationsdienste nutzen, deren Daten von der Funk- und Kabelaufklärung erfasst sein können. Darüber hinaus bestehen spezifische Umstände, welche die Wahrscheinlichkeit für die BeschwerdeführerInnen, von der Funk- und Kabelaufklärung erfasst zu werden, erhöhen (dazu nachstehend Ziff. 40.). Wirksame Rechtsbehelfe bestehen wie dargelegt nicht.

25. Der Beschwerdegegner wirft den BeschwerdeführerInnen vor, sie hätten davon abgesehen, ein datenschutzrechtliches Einsichtsgesuch zu stellen und mit entsprechenden Einträgen ein schutzwürdiges Interesse zu dokumentieren. Dieses Argument wirkt reichlich sophistisch. Die BeschwerdeführerInnen hatten das Gesuch beim Beschwerdegegner gestellt und konnten gleichzeitig von sich aus keine Kenntnis darüber haben, in wie weit sie der Beschwerdegegner über sie Daten bearbeitet. In ihrem Gesuch ist ein spezifisches Datenauskunftsbegehren im Zusammenhang mit dem eigentlichen Gegenstand des Gesuchs enthalten gewesen (Ziff. 3 der Anträge). In der Beschwerde haben sie den entsprechenden Antrag wiederholt. Es wäre damit am Beschwerdegegner, Auskunft in allfällige die BeschwerdeführerInnen betreffende Daten zu erteilen und zu belegen, dass durch die nachrichtendienstliche Tätigkeit, welche Gegenstand dieses Verfahrens ist, keine Grundrechte der BeschwerdeführerInnen verletzt werden. Hierzu gehört die Erteilung der Auskunft, ob und gegebenenfalls welche Daten der BeschwerdeführerInnen in den Informationssystemen des Beschwerdegegners gespeichert sind. Dies gehört zum Gegenstand des Verfahrens und kann nicht auf ein separat vom Beschwerdegegner behandeltes Datenauskunftsverfahren verschoben werden. Zudem zielt das von den BeschwerdeführerInnen gestellte Auskunftsbegehren nicht nur auf jene Daten, welche in den Informationssystemen des Beschwerdegegners gespeichert und mit den BeschwerdeführerInnen verknüpft sind. Die Überwachung und Datenbearbeitung durch den Beschwerdegegner, einschliesslich der Tätigkeit des ZEO, beginnt nicht erst mit der Speicherung von Daten in einem Informationssystem, sondern setzt wie dargelegt ein, sobald Kommunikationsdaten der BeschwerdeführerInnen im Rahmen der Funk- oder Kabelaufklärung gescannt werden. Das Auskunftsbegehren richtet sich demnach auch auf diese Datenverarbeitung und ebenso auf eine allfällige daran anschliessende weitere Speicherung und Bearbeitung.

26. Der Beschwerdegegner gibt in seiner Stellungnahme gleichzeitig an, Abklärungen des Beschwerdegegners in der einschlägigen Datenbank hätten ergeben, dass keiner der BeschwerdeführerInnen beim Beschwerdegegner im Zusammenhang mit einem Funk- und Kabelaufklärungsauftrag verzeichnet sei. Diese Auskunft deckt die mit der

Funk- und Kabelaufklärung verbundene Überwachung und Datenbearbeitung jedoch, wie sich aus den Darlegungen der BeschwerdeführerInnen ergibt, nur zu einem Teil ab. Mit der Auskunft, keiner der BeschwerdeführerInnen sei beim Beschwerdegegner im Zusammenhang mit einem Funk- und Kabelaufklärungsauftrag in der einschlägigen Datenbank verzeichnet, sind somit weder das Gesuch bzw. die Beschwerde noch das Interesse auf Datenauskunft gegenstandslos geworden. Die Problematik liegt hier nicht darin, dass die BeschwerdeführerInnen kein separates Datenauskunftsbegehren eingereicht haben, sondern darin, dass sie nach wie vor von der Funk- und Kabelaufklärung betroffen sind und der Beschwerdegegner sie weder von der Funk- und Kabelaufklärung ausnehmen noch darüber Auskunft geben kann, in wie weit im Rahmen der Funk- und Kabelaufklärung eine Bearbeitung und/oder Speicherung von sie betreffenden Daten stattgefunden hat.

27. Der Beschwerdegegner führt aus, wie ein genehmigter Auftrag durchgeführt wird. Ein Stück weit erscheinen diese Ausführungen durchaus als instruktiv. Es ist aber doch darauf hinzuweisen, dass damit in einigen wesentlichen Aspekten ein irreführendes Bild vermittelt wird, insbesondere was die Architektur des Netzwerkes betrifft, auf welchem das Internet aufbaut, und wie die Kabelaufklärung auf den Datenfluss zugreifen kann. Der Beschwerdegegner schreibt:

> *«Nach erfolgter Beauftragung ergeht durch das ZEO eine rechtsgültige Anordnung an den betreffenden Fernmeldedienstanbieter zur Ausleitung von Signalen. Beim ZEO wird laufend eine Statistik über den ausgeleiteten Verkehr erstellt. Dabei werden aber keine Daten gespeichert oder bereits an den NDB weitergeleitet. Anhand dieser Statistiken entscheidet das ZEO, welche der ausgeleiteten Fasern am vielversprechendsten sind und auch ob Fasern zum Beispiel nur inländischen Verkehr enthalten, welcher gar nicht verwendet werden darf. Beispielsweise wird festgestellt, dass auf einer Faser viel Verkehr aus Syrien durchläuft. Diese Faser wird dann weiterbearbeitet. Durch diesen Schritt wird die Menge der Daten noch einmal massiv reduziert (die Erfassung von rein inländischem Verkehr wird im Übrigen bereits durch die Auswahl der richtigen Ausleitungspunkte minimiert).*
>
> *Die auf den ausgewählten Fasern enthaltenen Daten werden nach den im Kabelaufklärungsauftrag definierten Kategorien von Suchbegriffen (beispielsweise Telefonnummern, IP Adressen, Schlüsselwörter) durchsucht und durch einen*

Analysten des ZEO ausgewertet. Dabei wird durch den Analysten noch einmal sichergestellt, dass die an den NDB weitergeleiteten Informationen auftragskonform sind oder direkte Hinweise auf eine Gefährdung der inneren oder äusseren Sicherheit enthalten und keine rein schweizerische Kommunikation enthalten (entsprechende Daten müssen vom ZEO vernichtet werden).»

28. Diese Darlegungen sind mit den tatsächlichen Gegebenheiten nicht in Übereinklang zu bringen. Dies wird deutlich, wenn man sich den Aufbau des Internets vor Augen hält: Das Internet ist ein weltweites Netzwerk aus Netzwerken («Internet»), das eine paketvermittelte Kommunikation ermöglicht. Es basiert auf der Internetprotokollfamilie, die sich in vier Schichten (Layer) unterteilen lässt: Link Layer, Internet Layer, Transportlayer und Anwendungsschicht (vgl. https://en.wikipedia.org/wiki/Internet_protocol_suite; https://de.wikipedia.org/wiki/Internetprotokollfamilie).

a) Link Layer (Kommunikation von a nach b)

Auf der untersten Schicht, dem Link Layer, findet die Kommunikation innerhalb eines Netzwerkes statt: beispielsweise in einem WLAN- oder in einem kleinen, nicht weiter unterteilten Firmennetzwerk. Findet bei der Übertragung ein Wechsel der physischen Übertragungstechnologie (ADSL, Cable, WLAN, Ethernet, Funk etc.) statt, stellt dies auch die technische Grenze eines Netzwerkes auf Ebene des Link Layers dar. Eine Glasfaser ist daher typischerweise ebenfalls ein «Netzwerk» auf dem Link Layer.

Internationale Glasfasern werden z. B. von Interoute (https://www.interoute.de/netzwerk), Level3/Centurylink (http://www.centurylink.com/asset/business/enterprise/brochure/centurylink-dark-fiber-br180090.pdf), Zayo (https://www.zayo.com/solutions/global-network/), COLT (https://www.colt.net/colt-network-map/) oder Telia (https://www.teliacarrier.com/Network-map.html) gebaut und überqueren auf Hochspannungsleitungen, entlang von Gaspipelines, Eisenbahnlinien oder Autobahnen weite Strecken. Kontinente werden durch Seekabel verbunden (http://cablemap.info/). Ein Glasfaserkabel besteht dabei in der Regel aus mehreren Fasern. In einem Kabel ist dann (in einem fiktiven Schweizer Beispiel) z. B. die Faser 1/2 (jeweils zwei zur Ausfallsicherheit) an AT&T vermietet, Faser 3/4 wird von Init7 beleuchtet, Faser 5/6 von Solnet, Faser 7/8 braucht die Anbieterin selber, während die Fasern 9 bis 144 (noch) unbenutzt sind.

Die Faser 7/8 könnte dann weiter (per DWDM) gemultiplext sein; sie würde also weiter nach Wellenlängen bzw. Farben unterteilt: Farbe «1» wäre dann z. B. an Quickline vermietet, Farbe «2» an Vodafone, Farbe «3» gekündigt, Farbe «4» von Netplus genutzt und die Farben 5 bis 32 noch frei.

Gemäss Botschaft zum Nachrichtendienstgesetz (19. Februar 2014, Seite 77) müssen «nur Betreiberinnen, die öffentliche Leistungen im Sinne des Fernmeldegesetzes vom 30. April 1997 (FMG) im grenzüberschreitenden Verkehr anbieten» Signale an den durchführenden Dienst liefern. Wobei das Fernmeldegesetz die «fernmeldetechnische Übertragung von Informationen» (Art. 2) regelt und diesen Vorgang als «elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk» (Art. 3) definiert. Aus Sicht des Nachrichtendienstgesetzes wären die Betreiberinnen der physischen Glasfaserkabel als die entsprechenden «Betreiberinnen von leitungsgebundenen Netzen» anzusehen.

b) Internet Layer (Kommunikation von a nach n)

Der Internet Layer sorgt übergeordnet dafür, dass Netzwerke basierend auf dem Link Layer miteinander verknüpft werden können – indem Datenpakete von einem in ein nächstes Netzwerk weitervermittelt werden. Die Aufgabe dieser Schicht ist es, zu einem empfangenen Paket das nächste Zwischenziel zu ermitteln und das Paket dorthin weiterzuleiten. Dieses Routing basiert auf IP-Adressen (Internet-Protokoll-Adressen) und Routingtabellen.

IP-Adressen werden global vergeben und können nicht zuverlässig einem Land zugeordnet werden (speziell bei international tätigen Organisationen und Providern). Die Routingtabellen ändern sich fortlaufend. Des Weiteren kann ein Ziel meist auch über mehrere Pfade erreicht werden («Multipath»). Dies kann dazu führen, dass zwei Teile einer Nachricht über unterschiedliche Routen, und somit über verschiedene Links, geschickt werden.

Auf dem Link Layer findet auch die Verknüpfung von Netzwerken unterschiedlicher Anbieter oder Organisationen statt («Peering» oder «Interkonnektion»). Eine Verbindung kann dabei individuell direkt geschaltet werden, oder sie findet an spezialisierten Internet Exchanges statt. In Europa befinden sich die grössten Internet Exchanges (https://www.pch.net/ixp/dir) in Frankfurt, Amsterdam, London und (bereits deutlich kleiner) Paris. Hier findet auch der interkontinentale Austausch der Daten statt, die meist per Seekabel übertragen werden. An den kleineren Internet Exchanges, wie in Zürich oder Genf, schliessen sich lokale Anbieter zusammen. Internationaler Traffic wird über angemietete Leitungen oder

Transportkapazitäten («IP Transit») zu den nächstgrösseren Internet Exchanges weitergeleitet.

Bei international tätigen Providern, resp. Konzernen, wie z.B. UPC Cablecom, die sowohl Endkundenschlüsse in der Schweiz anbieten aber auch ein eigenes internationales Netzwerk betreiben, ist es nicht unüblich, dass eigentlich lokaler Traffic über internationale Leitungen zu anderen Schweizer Provider geroutet wird. Auch im Fehlerfall oder Überlast können alternative Routen für lokalen Traffic über das Ausland führen. Ein Teil der Infrastruktur befindet sich oft ebenfalls im Ausland: So sind die Mailserver der Schweizer Kunden von UPC Cablecom in Österreich. Die Kommunikation findet entsprechend grenzüberschreitend statt.

c) Transportschicht

Die Transportschicht ermöglicht eine Ende-zu-Ende-Kommunikation der beteiligten Geräte. Sie ist im hier zu erläuternden Zusammenhang nicht weiter relevant.

d) Anwendungsschicht

Darauf aufbauend und auf Basis der unzähligen Protokolle der Anwendungsschicht kommunizieren nun die Internetanwendungen. So ermöglicht das Protokoll «SMTP» die Übertragung einer E-Mail an den eigenen Mailprovider, der wiederum die Mail an den Mailprovider des Empfängers weiterleitet, von wo es per HTTP, IMAP oder POP vom Empfänger abgerufen werden kann.

Es findet also keine direkte Kommunikation zwischen Absender und Empfänger einer Nachricht statt: Der Weg, den eine E-Mail macht, ist vielmehr von den verwendeten Mail-Providern und deren Server-Standorten abhängig. Die Server von GMX stehen z. B. in Deutschland, die Datacenter von Google/Gmail (https://www.google.com/about/datacenters/inside/locations/index.html), Outlook/Microsoft und iCloud/Apple sind rund um den Erdball verteilt, während Yandex wiederum Server in Finnland betreibt.

Zu erwähnen ist in diesem Zusammenhang auch die Telefonie, welche auch zunehmend IP-basiert funktioniert (IP-Telefonie, VoIP, SIP-Telefonie). Auch herkömmliche Telefonie-Anbieter haben auf IP-Telefonie umgestellt oder sind daran, umzustellen (so auch die Swisscom: *«Seit 2017 telefonieren alle Swisscom Kunden über das Internet mit der sogenannten Festnetz-Telefonie (IP)»* [https://www.swisscom.ch/de/privatkunden/hilfe/festnetz/ip-telefonie.html]). IP-Telefonie ist oftmals unverschlüsselt. Je nach Telefonie-Anbieter und je nach Standort der Person, welche IP-

Telefonie nutzt (etwa über ein Softphone von einem anderen Land aus als dem Land, in welchem sich der Serverstandort des Telefonie-Anbieters befindet) generiert IP-Telefonie grenzüberschreitenden Verkehr, welcher Ziel von Funk- und Kabelaufklärung sein kann.

Hervorzuheben ist noch der Umstand, dass bei der Kommunikation der Internetanwendungen Inhaltsdaten anfallen, aber auch Metadaten (angefangen bei der IP-Adresse der Datenpakete). Die bei der Funk- und Kabelaufklärung verwendeten Suchbegriffe können sich auf Inhalts- wie auf Metadaten beziehen. Die reine Analyse von Metadaten ist also auch Bestandteil der Funk- und Kabelaufklärung.

29. Die Kabelaufklärung setzt physisch auf der untersten Schicht an, dem Link Layer, und zwar an der Stelle, an dem ein Glasfaserkabel terminiert wird, also am Ende eines Glasfaserkabels an dessen Übergang zu anderen Datenleitungen. Ausgeleitet werden primär Signale einer Faser, welche in die Schweiz hinein bzw. aus der Schweiz heraus führt. Es stellt sich die Frage, welche Informationen aus den ausgeleiteten Signalen effektiv gewonnen werden kann, insbesondere mit Blick auf den Standort der Kommunikationsteilnehmer.

30. Es ist auf den unteren Schichten (und für die Betreiber von Glasfaserkabeln) weder ersichtlich, wo «viel Verkehr aus Syrien durchläuft» (vgl. Ausführungen des Beschwerdegegners), noch erschliesst sich dies aus der Überwachung der Datenpakete auf der Anwendungsschicht: Selbst E-Mail-Adressen haben einen höchst ungenauen Bezug zu einer Region; bei anderen Protokollen fehlt dieser komplett. Dies betrifft auch dezidierte Kommunikationsanwendungen: So wurde z.B. bekannt, dass der «Islamische Staat» Propagandakanäle im Messenger «Telegram» betrieben hat. Der Sitz des Unternehmens ist in Dubai. Die Server sind auf «different parts of the world» verteilt (https://core.telegram.org/api/datacenter), und stehen z. B. in London und Singapur (https://en.softonic.com/articles/telegram-secret-chats). Die Benutzernamen («E-Mail-Adressen») sind dabei frei wählbar.

31. Der vom NDB verwendete Lageradar «für die Darstellung der für die Schweiz relevanten Bedrohung» (Beilage 1, she. auch https://www.newsd.admin.ch/newsd/message/attachments/48133.pdf, S. 11) zeigt Arbeitsgebiete des NDB, die geografisch nicht eingegrenzt werden können, wie Cybernachrichtendienst, organisierte Kriminalität, Bedrohungen kritischer Infrastrukturen, nukleare Bedrohung, Terrorismusfinanzierung, Rechtsextremismus, Tierrechtsextremismus oder Cyberaktivismus. Aber auch die Bedrohungen, welche einer Region zugeordnet werden könnten, sind weit über den Erdball verteilt: Türkei, China, Nordafrika, Sri Lanka, Russland, USA, Nordkorea. Die im Lageradar verwendeten Arbeitsgebiete lassen sich grundsätzlich verschiedenen Zwecken, denen die Funk- und Kabelaufklärung dienen soll, zuordnen, so

insbesondere den Zwecken in den Bereichen Terrorismus sowie Aufklärung der Cyber-Bedrohung und Schutz kritischer Infrastrukturen (vgl. insb. Art. 25 NDV). Insbesondere das Arbeitsgebiet Cyberaktivismus wird damit auch Gegenstand der Funk- und Kabelaufklärung sein.

32. Gemäss Nachrichtendienstverordnung müssen die «Betreiberinnen von leitungsgebundenen Netzen» nun «dem ZEO Zutritt zu den für die Kabelaufklärung benötigten Räumen [gewähren], um die Installation von technischen Komponenten zu ermöglichen, die für die Durchführung von Kabelaufklärungsaufträgen notwendig sind» (Art. 28 NDV).

33. Art. 42 Abs. 2 NDG «stellt [dabei lediglich] sicher, dass keine rein schweizerischen Kommunikationen erfasst werden. Wo dies technisch nicht möglich ist (z.B. kann der Leitweg von IP-Datenpaketen nicht vorausgesagt werden, auch wenn sich Absender/in und Empfänger/in in der Schweiz befinden), sind solche Daten unverzüglich zu vernichten, sobald ihre schweizerische Herkunft und Zieladresse erkannt werden.» (vgl. Botschaft zum Nachrichtendienstgesetz, S. 75).

34. Befinden sich folglich aber entweder Sender und/oder Empfänger (IP-Adressen) im Ausland, so ist die Verwendung der erfassten Signale durch das ZEO zulässig: «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 an den Nachrichtendienst unverändert weiter.» (Art. 42 Abs. 3 NDG).

35. Aus der Betrachtung der Architektur des Internets und des Bedrohungsbilds des NDB erscheint das skizzierte Bild der Überwachung «einer Faser [auf der] viel Verkehr aus Syrien durchläuft» unzulässig vereinfacht und irreführend. Vielmehr lässt sich festhalten:

- Grenzüberschreitende Daten sind überwiegend Daten von Personen in der Schweiz an Dienste im Ausland (oder umgekehrt);

- in den allermeisten Fällen befindet sich bei einer grenzüberschreitenden Internet-Kommunikation prima vista immer eine IP-Adresse im Ausland und eine in der Schweiz;

- welche Personen effektiv von wo aus miteinander kommunizieren steht allein damit noch nicht fest;

- eine weitere geografische Eingrenzung der an einer Kommunikation beteiligten Personen ist kaum möglich und aus Sicht der relevanten Bedrohungen des Nachrichtendienstes letztlich auch nur begrenzt sinnvoll.

36. 2003 veröffentlichte die Geschäftsprüfungsdelegation der eidgenössischen Räte einen Bericht über das bereits bestehende, damals aber erst seit drei Jahren in Betrieb befindliche Satellitenaufklärungssystem «Onyx». Zum Zeitpunkt der Untersuchung durchsuchte die Überwachungsanlage die übertragenen Daten auf der Basis von rund dreissig Aufträgen nach je zwischen fünf und mehreren Hundert Schlüsselwörtern (https://www.admin.ch/opc/de/federal-gazette/2004/1499.pdf, S. 19 ff.).

37. Der Wert der Überwachung des Internets dürfte um ein Vielfaches grösser sein. So steht im Büchlein zur Volksabstimmung vom 25. September 2015 (S. 25): «Zur Beschaffung von Informationen über das Ausland sieht das Nachrichtendienstgesetz neben der Funk- und Satellitenaufklärung neu auch die Kabelaufklärung vor. Damit soll in grenzüberschreitenden Kabelnetzen nach Informationen gesucht werden, die für die Sicherheit der Schweiz von Bedeutung sind. Diese Ausdehnung ist erforderlich, weil die internationale Kommunikation immer weniger über Satelliten abgewickelt wird. Die Kabelaufklärung erhöht unter anderem die Chancen, elektronische Spionage fremder Staaten gegen die Schweiz oder Hackerangriffe zu erkennen.»

38. Damit wird das Bedrohungsbild auch über die «reine» Informationsgewinnung aus der Rasterung von Kommunikationsinhalten hinaus auf die Erkennung von ungewöhnlichen Vorgängen (mögliche Angriffe) auf Endpunkte in der Schweiz erweitert.

39. Die vom Beschwerdegegner skizzierte Eingrenzung der überwachten Datenströme und geografische Zuordnung der Kommunikationsteilnehmer funktioniert also nicht wie vom Beschwerdegegner suggeriert. Es ist kaum zielführend, auf die vom Beschwerdegegner beispielhaft beschriebene Art und Weise eine Faser zu suchen, über welche viel Verkehr aus Syrien läuft. Es ist auch nur sehr begrenzt möglich, rein inländischen Verkehr zu erkennen und dessen Erfassung durch die Wahl der richtigen Ausleitungspunkte oder durch die Wahl der Kategorien von Suchbegriffen zu minimieren.

    Nachdem der Beschwerdegegner wie dargelegt irreführende und falsche Aussagen zur Funktionsweise des Internets und zur Analyse der ausgeleiteten Kommunikation gemacht hat, insbesondere was die Geolokalisation betrifft, wird **beantragt**, ein Sachverständigengutachten bei einer Fachperson einzuholen zur Funktionsweise und Architektur des Internets sowie allgemein zur Funktionsweise und Architektur der von der Funk- und Kabelaufklärung erfassbaren Netzwerke und zur Thematik, an welchen Punkten die Funk- und Kabelaufklärung Daten ausleiten kann und wie sich die Wahl des Punktes, an dem Daten ausgeleitet werden darauf auswirkt, welche Daten anfallen und welche Analysemöglichkeiten sich aus diesen Daten ergibt, insbesondere was den Standort der involvierten Kommunikationspartner betrifft.

40. Wie bereits in der Beschwerdeschrift dargelegt sind die BeschwerdeführerInnen über die dargelegten allgemeinen Aspekte hinaus spezifisch von der Funk- und Kabelaufklärung betroffen. Nachdem der Beschwerdegegner die Legitimation der BeschwerdeführerInnen nach wie vor anzweifelt, sei in dieser Stellungnahme Folgendes ergänzt:

41. Die Beschwerdeführerin 1 ist ein gemeinnütziger Verein mit Sitz in Basel. Der Vorstand, die Geschäftsleitung und die Mitglieder teilen in ihrer Tätigkeit für den Verein vertrauliche Informationen mit Personen und Organisationen, welche sich mit der Beschwerdeführerin 1 austauschen, insbesondere mit Anwälten, Journalistinnen und Bürgerrechtsorganisationen, sowohl in der Schweiz wie auch international. Sie beraten und schulen auch Redaktionen, Unternehmen und Organisationen im Bereich der sicheren und vertraulichen Kommunikation.

42. Die Beschwerdeführerin 1 besitzt oder mietet keine Räumlichkeiten. Die Kommunikation, der Informationstausch, die Dateiablage etc. findet vorwiegend über das Internet statt. Die vom Verein betriebene und benutzte Infrastruktur (E-Mail, Mailinglisten, Mitgliederverwaltung, Dateiablage, Kollaborationstools) befindet sich verteilt in Deutschland, der Schweiz und Österreich. Das Büro ist sozusagen das Internet. Das Telefon-Gataway ist ein SIP-Account in der Schweiz, der häufig auch aus dem Ausland benutzt wird. Die Kommunikation findet entsprechend häufig grenzüberschreitend statt.

43. Die Beschwerdeführerin 1 beschäftigt sich mit den Auswirkungen der Digitalisierung und Vernetzung auf die Gesellschaft. Hierzu gehören nach dem Lageradar des NDB auch Cybernachrichtendienst, Überwachung (ausländischer Staatsbürger in der Schweiz), Cyberoperationen in Konflikten, Cyberaktivismus – insbesondere auch in der Türkei, in China und in Nordafrika.

44. Die Kommunikation kann also nicht nur inhaltlich vom ZEO verwendet und ausgewertet werden, es besteht auch eine reale Gefahr, dass vom NDB definierte Schlüsselwörter zu Treffer führen, dass die aus der betreffenden Kommunikation stammenden Daten gespeichert und bearbeitet werden und dass die Kommunikation der Beschwerdeführerin 1 weiter überwacht wird.

45. Der Beschwerdeführer 2 lebt in der Schweiz. Er kommuniziert sowohl geschäftlich als auch im Rahmen seines ehrenamtlichen zivilgesellschaftlichen Engagements viel auf elektronischem Weg mit ausländischen Kommunikationspartnern. Er nutzt Kommunikationsinfrastruktur und -Dienste (Email, Telefonie, Messenger, Kollaboration) in der Schweiz und international. Er ist geschäftlich und privat viel auf Reisen.

46. Der Beschwerdeführer 2 ist Vereinspräsident der Digitalen Gesellschaft. Er engagiert sich zudem ehrenamtlich zivilgesellschaftlich im Rahmen der internationalen Just Net Coalition, die sich im Internet-Kontext für Menschenrechte und soziale Gerechtigkeit einsetzt.

47. Einige Aktivitäten beider Organisationen dürften als «Cyberaktivismus» bezeichnet werden (vgl. «Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema Cyberaktivismus und zivilgesellschaftliche Organisationen» vom 16. September 2015). Der NDB ordnet einerseits «Cyberaktivismus» in die Kategorie «Extremismus» ein. Andererseits lässt es sich in internationalen zivilgesellschaftlichen Netzwerken nicht vermeiden, mit anderen zivilgesellschaftlichen Akteuren zu interagieren, die z.T. extremere Ansichten haben, oder die Formen des Cyberaktivismus praktizieren, die nicht notwendigerweise gutgeheissen werden müssen .

48. Die Kommunikation kann also nicht nur inhaltlich vom ZEO verwendet und ausgewertet werden, es besteht auch eine reale Gefahr, dass vom NDB definierte Schlüsselwörter (auch Personennamen von Kommunikationspartnern im Ausland) zu Treffern führen, dass die aus der betreffenden Kommunikation stammenden Daten gespeichert und bearbeitet werden und dass die Kommunikation weiter überwacht wird.

49. Der Beschwerdeführer 3 ist Informatiker und Geschäftsleiter der Beschwerdeführerin 1. Er benutzt das Internet tagtäglich für seine Arbeit und privat. Er besitzt verschiedenste E-Mail-Accounts in der Schweiz und Deutschland. Sein Telefon-Anschluss führt über das Internet. Er ist oft selber geschäftlich oder privat auf Reisen. Die Kommunikation findet entsprechend häufig grenzüberschreitend statt.

50. Grenzüberschreitende Kommunikation kann vom ZEO untersucht und nach Stichworten gerastert werden. Auch wenn daraus keine konkreten Treffer resultieren sollten, stellt dies eine Überwachung dar. Wer befürchtet oder weiss, überwacht zu werden, wird sein Kommunikationsverhalten und seinen Bewegungsfreiraum einschränken («chilling effect»). Freie Meinungsäusserung, Versammlungsfreiheit, schlussendlich Teilhabe an demokratischen Prozessen sind beeinträchtigt.

51. Der Beschwerdeführer 3 wird durch die Funk- und Kabelaufklärung in der Ausübung seiner Grundrechte erheblich und nachhaltig tangiert. Dies betrifft auch seine Tätigkeit als Geschäftsführer der Beschwerdeführerin 1, d.h. soweit die Beschwerdeführerin 1 durch die Funk- und Kabelaufklärung in ihren Grundrechten tangiert ist, betrifft dies im Wesentlichen auch den Beschwerdeführer 3 als die Person, welche konkret in die wesentlichen Aktivitäten der Beschwerdeführerin 1 involviert ist.

52. Die Kommunikation kann also nicht nur inhaltlich vom ZEO verwendet und ausgewertet werden, es besteht auch eine reale Gefahr, dass vom

NDB definierte Schlüsselwörter (auch Personennamen von Kommunikationspartnern im Ausland) zu Treffern führen , dass die aus der betreffenden Kommunikation stammenden Daten gespeichert und bearbeitet werden und dass die Kommunikation weiter überwacht wird.

53. Die Beschwerdeführerin 4 ist wie bereits dargelegt freischaffende Journalistin, Ko-Präsidentin des Recherche-Netzwerks investigativ.ch und Mitglied des «International Consortium of Investigative Journalists». Sie ist Beraterin und Mitarbeiterin beim «Investigative Reporting Project Italy». Neben ihrer Arbeit als Journalistin unterrichtet sie investigativen Journalismus und betreut StudentInnen.

54. Die Beschwerdeführerin 4 arbeitet vorwiegend in internationalen Recherche-Teams. Viele Personen befinden sich in den USA oder in Osteuropa. In ihrer journalistischen Tätigkeit teilt die Beschwerdeführerin vertrauliche Informationen mit ihren Kontakten per Email und Telefon über internationale Telekommunikationsverbindungen. So benutzt sie beispielsweise Email-Accounts in den USA, Signal, Skype und viele weitere Dienste, die im Ausland - also grenzüberschreitend - betrieben werden. Sie betreibt ein Kontaktformular in Österreich. Oft erhält sie über diese Kommunikationsmöglichkeiten vertrauliche Informationen von Informanten zugespielt.

55. Dem «International Consortium of Investigative Journalists» gehören 200 investigative Journalisten aus der ganzen Welt an. Viele Mitglieder arbeiten in gefährlichen Regionen oder an brisanten Themen. Die im Oktober 2017 in Malta durch eine Autobombe getötete Journalistin Daphne Galizia war eine von ihnen. Das ICIJ koordinierte zudem beispielsweise die einjährige Datenauswertung der «Panama Papers». Informationen werden oft per Email ausgetauscht.

56. Als Beraterin des «Investigative Reporting Project Italy» ist ihr Fokus «organisierte Kriminalität» (vrgl. Lageradar des NDB). Eine gemeinsame Recherche von IRPI und OCCRP hat im Februar 2018 mutmasslich das Leben des slovakischen Journalisten Jan Kuciak gekostet (https://www.occrp.org/en/amurderedjournalistslastinvestigation/). Die Beschwerdeführerin 4 steht mit weiteren Journalisten in Kontakt, die auf die organisierte Kriminalität in Europa spezialisiert sind.

57. Einer der Tätigkeitsschwerpunkte der Beschwerdeführerin 4 ist «Cybernachrichtendienst». Sie steht hierzu international mit verschiedenen Redaktionen und Journalisten in regelmässigem Kontakt. Weitere Tätigkeitsfelder sind Wirtschaftsspionage/Whistleblower, Graswurzelbewegungen/Linksextremismus, Cyberaktivismus sowie Cyberoperationen in Konflikten. Ihre Kommunikation kann also nicht nur inhaltlich vom ZEO ausgewertet werden, es besteht auch eine reale Gefahr, dass vom NDB definierte Schlüsselwörter zu Treffer führen, dass die aus der betreffenden Kommunikation stammenden Daten gespeichert

und bearbeitet werden und dass ihre Kommunikation weiter überwacht wird.

58. Die Beschwerdeführerin 5 ist wie bereits dargelegt Journalistin bei der Wochenzeitung WOZ. In ihrer journalistischen Tätigkeit teilt die Beschwerdeführerin vertrauliche Informationen mit ihren Kontakten per Email und Telefon auch über internationale Telekommunikationsverbindungen. So benutzt sie einen Email-Account bei GMX. Die Server stehen in Deutschland. Die Kommunikation findet also grenzüberschreitend statt.

59. Als Messenger nutzt sie Telegram und Signal. Auch hier stehen die Server im Ausland. Ihre grenzüberschreitende Kommunikation kann entsprechend vom ZEO erfasst und ausgewertet werden. Bekannt ist, dass auch der «Islamische Staat» Propagandakanäle im Messenger Telegram betrieben hat. Der Dienst dürfte von besonderem Interesse für die Geheimdienste sein.

60. Wie bereits ausgeführt, betrifft ein Tätigkeitsschwerpunkt der Beschwerdeführerin 5 das vom NDB als «Migrationsrisiken» bezeichnete Feld. In ihren Recherchen steht die Beschwerdeführerin in Kontakt u.a. mit Flüchtlingen, Behörden, Menschenrechtsorganisationen, PolitikerInnen und AnwältInnen, oft also mit Kontakten, die besonders exponiert sind und/oder Berufsgeheimnissen unterliegen. Die Recherchen der Beschwerdeführerin 5 umfassen auch Dschihad-Reisende und mögliche «IS-Zellen» in der Schweiz (https://www.woz.ch/-6506; https://www.woz.ch/-7256).

61. Ihre Kommunikation kann also nicht nur inhaltlich vom ZEO ausgewertet werden, es besteht auch eine reale Gefahr, dass vom NDB definierte Schlüsselwörter zu Treffer führen, dass die aus der betreffenden Kommunikation stammenden Daten gespeichert und bearbeitet werden und dass ihre Kommunikation weiter überwacht wird. Sie ist essenziell darauf angewiesen, dass der Schutz ihrer journalistischen Quellen gewährleistet ist.

62. Der Beschwerdeführer 6 ist wie bereits dargelegt Journalist bei Netzpolitik.org in Berlin. Das Medium trägt massgeblich zu einer transparenten Politik in der Bundesrepublik Deutschland und darüber hinaus bei. So werden regelmässig Regierungsdokumente publiziert und z.B. aus dem NSA-Untersuchungsausschuss berichtet, zu dem es ansonsten keine öffentliche Protokolle gibt.

63. In seiner journalistischen Tätigkeit teilt der Beschwerdeführer 6 vertrauliche Informationen mit seinen Kontakten per Email, Messenger und Telefon über internationale Telekommunikationsverbindungen. So benutzt er beispielsweise einen Email- und einen XMPP-Account (Messenger) bei einem Schweizer Anbieter. Die Kommunikation findet also in der Regel

grenzüberschreitend Deutschland-Schweiz statt. Zudem befindet er sich oft in Ländern, die gemäss dem Lageradar ein Überwachungsziel des NDB sind, wie beispielsweise die Türkei oder Russland. Seine grenzüberschreitende Kommunikation kann entsprechend vom ZEO erfasst und ausgewertet werden.

64. Der Beschwerdeführer 6 arbeitet mit Bürgerrechtsorganisationen in westlichen Demokratien wie auch in repressiven Staaten oder gar Bürgerkriegsregionen zusammen. So hat er, wie bereits ausgeführt, den Aufbau des syrischen Überwachungsstaates und die Verstrickung westlicher Firmen gemeinsam mit Privacy International dokumentiert [https://netzpolitik.org/?p=141138]. Er unterhält vielfältig Kontakte von und nach Interessensgebieten (und in Überschneidung mit den Aufklärungsszielen des NDB), wie China, Nordafrika, Syrien, Irak oder Russland. Er beschäftigt sich mit «Migrations-Risiken», «Cyberaktivismus», «Cyberoperationen in Konflikten» und «Cybernachrichtendienst». Seine Kommunikation kann also nicht nur inhaltlich vom ZEO ausgewertet werden, es besteht auch eine reale Gefahr, dass vom NDB definierte Schlüsselwörter zu Treffer führen, dass die aus der betreffenden Kommunikation stammenden Daten gespeichert und bearbeitet werden und dass seine Kommunikation weiter überwacht wird.

65. In seiner journalistischen Tätigkeit ist der Beschwerdeführer essenziell darauf angewiesen, dass der Schutz seiner journalistischen Quellen gewährleistet ist. Erschwerend wirkt, dass die mittels der Funkaufklärung empfangenen Informationen auch ein nützliches «Tauschmittel» mit den entsprechenden Dienststellen im Ausland, wie beispielsweise dem Verfassungsschutz der Bundesrepublik Deutschland, bilden (vgl. GPDel-Bericht vom 10. November 2003, Ziff. 5.3). Dass dies eine reale Bedrohung ist, zeigt das Ermittlungsverfahren wegen Landesverrats im Jahr 2015.

66. Der Beschwerdeführer 7 ist wie dargelegt Politikwissenschaftler und Journalist. Die Schwerpunkte seiner Tätigkeit sind in der Beschwerde dargelegt worden. Er ist damit aufgrund seiner Tätigkeit insbesondere in dem vom NDB als «Migrationsrisiken» bezeichneten Feld sowie in den Bereichen «Cyberaktivismus», «Cyberoperationen in Konflikten» und «Cybernachrichtendienst» tangiert. Dadurch, dass er sowohl in der Schweiz als auch in Deutschland tätig ist mit Personen und Organisationen in verschiedenen Ländern kommuniziert, insbesonder per Email und Telefon, generiert er Datenverkehr, welcher vom NDB als grenzüberschreitend qualifiziert wird.

67. Seine Kommunikation kann also nicht nur inhaltlich vom ZEO ausgewertet werden, es besteht auch eine reale Gefahr, dass vom NDB definierte Schlüsselwörter zu Treffer führen, dass die aus der betreffenden Kommunikation stammenden Daten gespeichert und bearbeitet werden und dass seine Kommunikation weiter überwacht wird. Er ist essenziell

darauf angewiesen, dass der Schutz seiner journalistischen Quellen gewährleistet ist.

68. Der Beschwerdeführer 8 ist als Rechtsanwalt tätig. Aufgrund der in der Beschwerdeschrift beschriebenen Tätigkeitsbereiche ist er von verschiedenen Feldern, welche im Fokus des NDB stehen, tangiert, insbesondere in dem vom NDB als «Migrationsrisiken» bezeichneten Feld sowie in weiteren in den Bereichen Terrorismus und Extremismus subsumierten Feldern.

69. Seine Kommunikation kann also nicht nur inhaltlich vom ZEO ausgewertet werden, es besteht auch eine reale Gefahr, dass vom NDB definierte Schlüsselwörter zu Treffer führen, dass die aus der betreffenden Kommunikation stammenden Daten gespeichert und bearbeitet werden und dass seine Kommunikation weiter überwacht wird. Werden ihn betreffende Daten erfasst, so greift dies auch in seine über das Berufsgeheimnis geschützte Tätigkeit als Rechtsanwalt ein und verletzt das durch das Berufsgeheimnis geschützte Verhältnis zwischen seinen Mandanten und ihm.

70. In der Beschwerdeschrift ist einlässlich dargelegt worden, dass die mit der Funk- und Kabelaufklärung verbundene Massenüberwachung nicht zu rechtfertigen ist und dass die BeschwerdeführerInnen durch die Funk- und Kabelaufklärung in ihren Grundrechten verletzt werden. Diese Schlussfolgerung ist vom Beschwerdegegner nicht entkräftet worden.

Mit freundlichen Grüssen

Viktor Györffy

Im Doppel

Beilagen:

1. Lageradar des NDB «für die Darstellung der für die Schweiz relevanten Bedrohung»
2. Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema Cyberaktivismus und zivilgesellschaftliche Organisationen vom 16. September 2015