Peyrot, Schlegel & Györffy
Rechtsanwälte

Zürich, 31. August 2017

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
Nachrichtendienst des Bundes NDB
Papiermühlestrasse 20
3003 Bern

Digitale Gesellschaft, 4000 Basel (Gesuchstellerin 1)
... (Gesuchsteller 2)
... (Gesuchsteller 3)
... (Gesuchstellerin 4)
... (Gesuchstellerin 5)
... (Gesuchsteller 6)
... (Gesuchsteller 7)
... (Gesuchsteller 8)

Sehr geehrte Damen und Herren

Namens und im Auftrag der eingangs genannten GesuchstellerInnen stelle ich Ihnen das

Gesuch

mit folgenden

Anträgen:

1. Der Betrieb der Funk- und Kabelaufklärung durch den NDB und weiteren Stellen, namentlich durch das Zentrum für elektronische Operationen der Armee (ZEO) sowie jegliche Tätigkeiten, die dem Betrieb der

Funkaufklärung und Kabelaufklärung dienen, seien zu unterlassen.

2. Der NDB habe jegliche in den Betrieb der Funk- und Kabelaufklärung involvierten Stellen und Personen anzuweisen, ihre diesbezügliche Tätigkeit zu unterlassen.

3. Es sei den GesuchstellerInnen mitzuteilen, ob und in welcher Weise Kommunikation von ihnen Gegenstand der Funk- oder Kabelaufklärung ist oder gewesen ist, und es sei ihnen mitzuteilen, welche sie betreffenden Daten, welche aus der Funk- oder Kabelaufklärung stammen, vom NDB oder vom ZEO bearbeitet werden, einschliesslich der Auskunft über weitere Daten, welche im Zusammenhang mit diesen aus der Funk- oder Kabelaufklärung stammenden Daten bearbeitet werden.

4. Es sei festzustellen, dass die Funk- und Kabelaufklärung die GesuchstellerInnen in ihren Grundrechten verletzt, namentlich in ihrem Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]), in ihrer Freiheit der Meinungsäusserung, der Meinungs- und Informationssowie die Medienfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II) und der Versammlungsfreiheit (Art. 22 BV, Art. 11 EMRK), in ihrer persönliche Freiheit und der Bewegungsfreiheit (Art. 10 Abs. 2 BV, Art. 8 EMRK) sowie ihre Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV).

5. Es sei festzustellen, dass die Funk- und Kabelaufklärung die GesuchstellerInnen 4, 5 und 6 als JournalistInnen in ihrem Anspruch auf

Medienfreiheit und auf Quellenschutz (Art. 17 BV und Art. 10 EMRK) verletzt.

6. Es sei festzustellen, dass die Funk- und Kabelaufklärung den Gesuchsteller 8 im Berufsgeheimnis als Rechtsanwalt und dadurch in seinem Recht auf Achtung des Privatlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]) und in seiner Wirtschaftsfreiheit (Art. 27 BV) verletzt;

unter Kosten- und Entschädigungsfolgen zu Lasten des Staates.

I. Formelles

1. Der unterzeichnende Rechtsanwalt ist zur Vertretung der GesuchstellerInnen gehörig bevollmächtigt. Eine Kopie der entsprechenden Vollmachten liegt dem Gesuch bei (s. **Beilagen 1 - 8**).

2. Wer ein schutzwürdiges Interesse hat, kann gemäss Art. 25a VwVG von der Behörde, die für Handlungen zuständig ist, welche sich auf öffentliches Recht des Bundes stützen und Rechte und Pflichten berühren, verlangen, dass sie (a.) widerrechtliche Handlungen unterlässt, einstellt oder widerruft und (b.) die Folgen widerrechtlicher Handlungen beseitigt.

3. Die Funk- und Kabelaufklärung beschlägt, wie nachstehend dargelegt wird, Grundrechte, welche durch die Europäische Menschenrechtskonvention (EMRK) geschützt sind. Damit muss – in Verbindung mit diesen Grundrechten – auch das Recht auf effektive Beschwerde gemäss Art. 13 EMRK gewahrt sein. Es sei diesbezüglich auf die Praxis des Europäischen Gerichtshofs für Menschenrechte (EGMR) zur Opfereigenschaft bei geheimdienstlichen Überwachungsmassnahmen verwiesen. Demnach kann ein Gesetz als solches die Rechte einer Person verletzen, wenn diese dadurch, ohne Vorliegen besonderer Durchführungsmassnahmen, unmittelbar betroffen ist. Die Konvention und ihre Organe sind zum Schutze des Einzelnen geschaffen worden, weshalb die Verfahrensvorschriften der Konvention in einer Art und Weise angewendet werden müssen, die dazu dient, das System der

Individualbeschwerde wirksam werden zu lassen. Eine Person kann unter gewissen Voraussetzungen geltend machen, sie sei durch die blosse Existenz geheimer Massnahmen oder der solche Massnahmen gestattenden Gesetze Opfer einer Verletzung der Konvention, ohne behaupten zu müssen, dass solche Maßnahmen tatsächlich gegen sie getroffen worden seien (vgl. die diesbezüglich mit der hier vorliegenden Konstellation vergleichbaren Entscheide 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.; 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.). Zur Wahrung des Rechts auf effektive Beschwerde ist das Gesuch damit von der zuständigen Behörde materiell zu behandeln und es ist dabei entweder gutzuheissen oder es ist den GesuchstellerInnen im Falle der Ablehnung die Möglichkeit zu gewähren, ein Rechtsmittel an eine Instanz zu ergreifen, welche die Sache wiederum materiell behandelt.

4. Die Funk- und Kabelaufklärung stellt einen erheblichen und unrechtmässigen Eingriff in die nachstehend (II.C.) genannten Grundrechte dar.

5. Die Funk- und Kabelaufklärung berührt somit Grundrechte der GesuchstellerInnen. Es handelt sich bei der Funk- und Kabelaufklärung mithin um eine Handlung i.S.v. Art. 25a VwVG.

6. Das erforderliche schutzwürdige Interesse der GesuchstellerInnen ergibt sich vorliegend ohne Weiteres daraus, dass für sie, wie nachstehend (II.C.) dargelegt, aus der Funk- und Kabelaufklärung schwere Eingriffe in Grundrechte, welche u.a. durch die EMRK geschützt sind, resultieren.

7. Die Gesuchstellerin 1 ist ein gemeinnütziger Verein mit Sitz in Basel. Der Zweckartikel (Art. 2) der Statuten der Digitalen Gesellschaft (s. **Beilage 9**) lautet wie folgt:

> *«Die Digitale Gesellschaft ist eine Bürgerrechts- und Konsumentenschutzorganisation mit gemeinnützigem Charakter. Der Verein setzt sich für Grund- und Menschenrechte, eine offene Wissenskultur sowie weitreichende Transparenz und Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen ein. Sein Ziel ist der Erhalt und die Förderung einer freien, offenen und nachhaltigen digitalen Gesellschaft auf dem Hintergrund der Persönlichkeits- und Menschenrechte.*
> *Die Zwecke des Vereins sind*
> - *Konsumentenberatung und Konsumentenschutz, insbesondere hinsichtlich der Nutzung von digitalen Netzen, Medien und Inhalten;*

- *Stärkung der Menschenrechte und des freiheitlich-demokratischen Staatswesens im digitalen Zeitalter, insbesondere durch den Einsatz für Meinungs- und Informationsfreiheit, für informationelle Selbstbestimmung und für den Schutz der Privatsphäre;*
- *Förderung von Bildung, Wissenschaft und Forschung, insbesondere auf den Gebieten Informatik, Kommunikationswissenschaften sowie Demokratie und Recht, soweit diese für die Freiheit, Offenheit und Nachhaltigkeit der Gesellschaft relevant sind.*

Dazu stellt er namentlich auch entsprechende Dienste der Öffentlichkeit zur Verfügung.
Der Verein kann diese Zielsetzungen in rechtlichen Verfahren jeder Art vertreten.
Der Verein folgt keinem kommerziellen Zweck und erstrebt keinen Gewinn. Er ist parteipolitisch und konfessionell neutral. Der Verein erfüllt seine Aufgaben objektiv und unabhängig, ohne Rücksicht auf bestimmte Unternehmungen, Organisationen oder Richtungen. Er kann gleichgerichtete Bestrebungen, namentlich auch solche der öffentlichen Hand, unterstützen und in geeigneter Weise mit entsprechenden Organisationen zusammenarbeiten.»

Die Prämbel der Statuten hält fest:

«Der Schutz der Privatsphäre im Internet ist ein hohes Gut und der Anspruch auf ungehinderte Kommunikation ein Menschenrecht. Vertraulichkeit und das aktive Recht, darüber zu bestimmen, welche Daten über sich von anderen genutzt werden und welche Informationen auf einen selbst einwirken dürfen, sind Kernbestandteile einer freien Gesellschaft. Sie bilden die Grundlage der informationellen Selbstbestimmung, des Datenschutzes, der Meinungs- und Informationsfreiheit. Die Digitale Gesellschaft setzt sich dafür ein, dass jede Person das Recht und die Möglichkeit behält, ihre digitalen Freiheitsrechte in dem Rahmen wahrzunehmen, der durch die internationalen Menschenrechtsrechte und die damit im Einklang stehenden nationalen Gesetzen definiert ist.»

Die Digitale Gesellschaft informiert sich regelmässig über Themen, welche im Fokus ihres Vereinszwecks stehen, und stellt diesbezügliche Informationen zur Verfügung, u.a. über ihre Website www.digitale-gesellschaft.ch. Die Digitale Gesellschaft und die für sie aktiven Mitglieder, insbesondere der Vereinsvorstand und ihr Geschäftsführer, stehen dabei in Kontakt mit verschiedenen Personen und Organisationen im In- und Ausland. Die Digitale Gesellschaft ist in ihrer Kommunikation und Information somit in vergleichbarer Weise von der Funk- und Kabelaufklärung betroffen wie die übrigen GesuchstellerInnen. Die Digitale Gesellschaft verfügt somit ebenfalls über ein schützenswertes Interesse mit Bezug auf das gestellte Gesuch. Ausserdem ist die Digitale Gesellschaft insoweit zur Führung dieses Verfahrens legitimiert, als es dabei statutengemäss die Interessen seiner Mitglieder wahrt, welche ebenfalls von der Funk- und Kabelaufklärung betroffen sind, sowie darüber hinaus allgemein die Interessen der in ihren Grundrechten betroffen Personen. Die Digitale Gesellschaft ist ein Verein von gesamtschweizerischer Bedeutung. Themen, mit denen sie sich befasst hat und befasst, sind von grundsätzlicher Bedeutung. Bei den entsprechenden Debatten und Gesetzgebungsverfahren in Medien und Politik hat sich die Digitale Gesellschaft aktiv beteiligt, insbesondere auch im Gesetzgebungsverfahren zum NDG. Die Digitale Gesellschaft pflegt dabei auch internationale Kontakte und ist im Rahmen ihrer Medienarbeit immer wieder mit JournalistInnen im Kontakt (s. www.digitale-gesellschaft.ch).

8. Welche Behörde für die zu beurteilenden Handlungen – und damit zur Behandlung des vorliegenden Gesuchs – zuständig ist, ergibt sich aus den anwendbaren Sach- und Organisationsgesetzen (vgl. ISABELLE HÄNER in: Praxiskommentar zum VwVG, Zürich 2009, Art. 25a, N 30). Gemäss NDG, NDV und VEKF ist der NDB Auftraggeber bei der Funk- und Kabelaufklärung und dafür verantwortlich, die entsprechenden Aufträge zu formulieren und die Genehmigung für deren Durchführung einzuholen. Ihm obliegt auch die weitere Bearbeitung der im Rahmen der Funk- und Kabelaufklärung gewonnenen Resultate. Der NDB ist somit sachlich und funktionell zur Behandlung des vorliegenden Gesuchs zuständig.

9. Sofern der NDB der Auffassung ist, er sei nicht für die Behandlung des Gesuches zuständig, wird er gestützt auf Art. 8 VwVG ersucht, das Gesuch an die zuständige Behörde weiterzuleiten und die GesuchstellerInnen darüber zu informieren.

II. Begründung

A. Einleitung

1. Nachstehend wird aufgezeigt, dass die Funk- und Kabelaufklärung zu schwer wiegenden Eingriffen in die Grundrechte der Gesuchsteller führt. Für diese Eingriffe besteht keine genügend bestimmte gesetzliche Grundlage. Der vorhandenen gesetzlichen Grundlage fehlt es an

hinreichender Klarheit. Die Auswirkungen der Funk- und Kabelaufklärung müssen aufgrund des Gesetzes hinreichend deutlich vorhersehbar sein. Dies ist bei den konkreten gesetzlichen Bestimmungen nicht der Fall. Die Eingriffe erscheinen nicht als verhältnismässig und gerechtfertigt.

2. Diese Beurteilung ergibt sich insbesondere aus der Praxis des EGMR zu den mit Massenüberwachungen verbundenen Grundrechtseingriffen und aus diesbezüglichen Reports des Office of the United Nations High Commissioner for Human Rights.

3. Die Funk- und Kabelaufklärung verletzt damit die Grundrechte der GesuchstellerInnen.

B. Gegenstand und gesetzliche Regelung der Funk- und Kabelaufklärung

1. Gemäss Art. 38 Abs. 1 NDG kann der Bund einen Dienst für die Erfassung elektromagnetischer Ausstrahlungen von Telekommunikationssystemen, die sich im Ausland befinden, betreiben (Funkaufklärung). Die Funkaufklärung dient gemäss Art. 38 Abs. 2 NDG der Beschaffung sicherheitspolitisch bedeutsamer Informationen über Vorgänge im Ausland, insbesondere aus den Bereichen Terrorismus, Weiterverbreitung von Massenvernichtungswaffen und ausländische Konflikte mit Auswirkungen auf die Schweiz sowie der Wahrung weiterer wichtiger Landesinteressen nach Art. 3 NDG.

2. Gemäss Art. 39 NDG kann der NDB den durchführenden Dienst damit beauftragen, zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland nach Art. 6 Abs. 1 Bst. b ND sowie zur Wahrung weiterer wichtiger Landesinteressen nach Art. 3 NDG grenzüberschreitende Signale aus leitungsgebundenen Netzen zu erfassen (Kabelaufklärung). Im Weiteren ist der Zweck der Funkaufklärung in Art. 25 NDV festgelegt. Befindet sich sowohl der Sender als auch der Empfänger in der Schweiz, so ist die Verwendung der nach Art. 39 Abs. 1 NDG erfassten Signale nicht zulässig. Kann der durchführende Dienst solche Signale nicht bereits bei der Erfassung ausscheiden, so sind die beschafften Daten zu vernichten, sobald erkannt wird, dass sie von solchen Signalen stammen (Art. 39 Abs. 2 NDG). Daten aus erfassten Signalen dürfen nur an den NDB weitergeleitet werden, wenn deren Inhalt den für die Erfüllung des Auftrags definierten Suchbegriffen entspricht. Die Suchbegriffe sind so zu definieren, dass ihre Anwendung möglichst geringe Eingriffe in die Privatsphäre von Personen verursacht. Angaben über schweizerische natürliche oder juristische Personen sind als Suchbegriffe nicht zulässig (Art. 39 Abs. 3 NDG). Aufträge zur Kabelaufklärung sind genehmigungspflichtig (Art. 40 NDG), entsprechend dem in Art. 41 NDG festgelegten Genehmigungsverfahren.

3. Bei der Funkaufklärung und bei der Kabelaufklärung werden Datenströme, welche mittels Funksignalen, namentlich über Satelliten, und mittels

Fernmeldekabeln übertragen werden, erfasst und nach Inhalten abgesucht, triagiert und der Auswertung zugeführt (vgl. Bericht zum Vorentwurf zum NDG vom 8. März 2013 [im Folgenden: Bericht zum Vorentwurf], S. 50, Botschaft zum NDG vom 19. Februar 201, BBl 2014, S. 2105 ff., [im Folgenden: Botschaft], S. 2178, sowie Berichte der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 10. November 2003 zum Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport [Projekt «Onyx»] und vom 9. November 2007 zur Rechtmässigkeit und Wirksamkeit des Funkaufklärungssystems «Onyx» [im Folgenden: Berichte GPDel vom 10. November 2003 bzw. vom 9. November 2007]). Funk- und Kabelaufklärung zielen damit nicht auf spezifische Kommunikationsvorgänge zwischen bestimmten Kommunikationsteilnehmern, vielmehr sollen Datenströme gesamthaft nach definierten Stichworten durchsucht werden. Das Zentrum für elektronische Operationen der Armee (ZEO) als durchführender Dienst durchsucht die Datenströme nach Stichworten und leitet die gewonnenen Informationen, die auf eine entsprechende Bedrohung hinweisen, an den NDB weiter. Die Funk- und Kalbelaufklärung erlaubt damit eine Art Rasterfahndung in den erfassten Datenströmen.

5. Jegliche Kommunikation, welche in den erfassten Datenströmen enthalten ist, wird damit von der Funk- bzw. Kabelaufklärung erfasst, um eruieren zu können, ob zuvor gesetzte Stichworte darin enthalten sind. Ist dies der Fall, wird die Kommunikation vertieft ausgewertet.

6. Diese Art von Rasterfahndung und die Durchsuchung und Auswertung anhand von Stichwörtern bringt es mit sich, dass nicht nur Kommunikation von Personen, von welchen eine einschlägige Bedrohung ausgeht, Bestandteil der Funk- und Kabelaufklärung wird, sondern potenziell jede Kommunikation, welche über Funksignale und Fernmeldekabel geführt sind, welche technisch in der Reichweite dieser Überwachungsmassnahme liegt. Der gesamte erfasste Datenstrom wird überwacht. Finden sich Stichwörter im Datenstrom (Hits), so wird die entsprechende Kommunikation vertieft betrachtet, wobei auch die Personen, welche die Hits generiert haben, wie nachstehend dargelegt (Ziff. 2.B.28.) konkret nicht unbedingt eine einschlägige Bedrohung darstellen. In den Hits wird sich vielmehr (auch) die Kommunikation völlig unbescholtener Personen finden.

7. Grundsätzlich kann jede Form von elektronischer Kommunikation Gegenstand der Funk- bzw. Kabelaufklärung sein. Das können etwa Daten sein aus der Nutzung von Internetdiensten wie WWW und E-Mail, Messenger-Diensten, aber auch Telefonie und Fax. Erfasst werden können sowohl Inhaltsdaten als auch Metadaten. Metadaten bilden keine Kommunikationsinhalte ab, können aber Hinweise auf die Kommunikationsteilnehmer geben, darauf, wo sich diese befinden, wann

und über welche Kanäle sie kommunizieren sowie weitere Umstände und Parameter der Kommunikation.

8. Mit der Funkaufklärung können Signale erfasst werden, welche in Reichweite entsprechender Anlagen in der Schweiz liegen, namentlich Satellitenkommunikationen, welche von Abhöreinrichtungen des Projekts Onyx erreicht werden können. Mit der Kabelaufklärung können die Datenströme abgegriffen werden, bei den Betreiberinnen von leitungsgebundenen Netzen und den Anbieterinnen von Telekommunikationsdienstleistungen i.S.v. Art. 43 NDG durchlaufen. Diese Betreiberinnen und Anbieterinnen haben dem NDB die für die Durchführung der Kabelaufklärung notwendigen technischen Angaben zu machen, und sie haben dem ZEO Zutritt zu den für die Kabelaufklärung benötigten Räumen zu gewähren, um die Installation von technischen Komponenten zu ermöglichen, die für die Durchführung von Kabelaufklärungsaufträgen notwendig sind (Art. 43 NDG, Art. 29 NDV).

9. Bei der heutigen Telekommunikation bestehen oft mehrere Möglichkeiten, welchen Weg Datenströme vom Sender zum Empfänger konkret nehmen. Über welche Infrastruktur die Datenströme laufen, ist nicht durchwegs eindeutig vorherbestimmt und vorhersehbar. Dies trifft insbesondere auf IP-basierte Kommunikation zu. Damit ist umgekehrt auch nicht eindeutig festgelegt oder vorhersehbar, was für Daten anfallen bzw. von welchen Absendern Daten stammen und wohin sie gehen sollen, wenn ein bestimmter Datenstrom mittels Funk- oder Kabelaufklärung durchsucht wird.

10. Verschiedene im NDG enthaltene Bestimmungen zielen darauf ab, die Erfassung «inländischer» Kommunikation durch Funk- und Kabelaufklärung einzuschränken. Die Funkaufklärung erlaubt die Erfassung elektromagnetischer Ausstrahlungen von Telekommunikationssystemen, die sich im Ausland befinden (Art. 38 Abs. 1 NDG). Der Bundesrat hat gemäss Art. 38 Abs. 4 lit. b. NDG sicherzustellen, dass der durchführende Dienst Informationen über Personen im Inland nur weiterleitet, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind und zuvor anonymisiert wurden. Die Kabelaufklärung soll grenzüberschreitende Signale aus leitungsgebundenen Netzen erfassen (Art. 39 Abs. 1 NDG). Befindet sich sowohl der Sender als auch der Empfänger in der Schweiz, so ist die Verwendung der erfassten Signale gemäss Art. 39 Abs. 2 NDG nicht zulässig. Angaben über schweizerische natürliche oder juristische Personen sind als Suchbegriffe nicht zulässig (Art. 39 Abs. 3 NDG letzter Satz). Kann der durchführende Dienst solche Signale nicht bereits bei der Erfassung ausscheiden, so sind die beschafften Daten zu vernichten, sobald erkannt wird, dass sie von solchen Signalen stammen. Informationen über Personen im Inland leitet der durchführende Dienst nur dann an den NDB weiter, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind und zuvor anonymisiert wurden (Art. 42 Abs. 2 NDG).

11. Diese Bestimmungen sind allerdings nur von beschränkter Wirkung. Die Erfassung von Kommunikation wird damit von vornherein nicht ausgeschlossen, soweit sich Sendern und Empfänger oder einer der beiden im Ausland befinden. Hinzu kommt, dass sich in vielen Fällen nicht feststellen lässt, wo sich Sender und Empfänger effektiv befinden. Bei Kommunikation über das Internet wird auf die Geolokalisation der IP-Adresse von Sender und Empfänger abgestellt. Diese IP-Adresse wiederspiegelt aber nicht unbedingt, wo sich Sender und Empfänger effektiv befinden. Werden etwa E-Mails erfasst, welche über einen sich im Ausland befindenden Mailprovider versendet oder empfangen werden, so wird dies als grenzüberschreitende Kommunikation gewertet werden, und zwar auch dann, wenn sich effektiv Sender und Empfänger in der Schweiz befinden, beispielsweise wenn eine Person, die in der Schweiz ist, über einen Mailaccount beim deutschen Anbieter GMX ein Mail an eine bluewin.ch-Mailadresse sendet. Dasselbe gilt für weitere Dienste, etwa bei der Nutzung von Messenger-Diensten. Grenzüberschreitende Kommunikation i.S.v. Art. 39 NDG liegt im Übrigen auch vor, wenn eine Person im Inland die Website einer Person oder eines Unternehmens im Inland aufruft, diese Website aber im Ausland gehostet wird.

12. Die Umsetzung der Bestimmung, wonach Informationen über Personen im Inland nur weitergeleitet werden, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind und zuvor anonymisiert wurden, setzt voraus, dass die Information zuvor durch eine entsprechende Auswertung einer Person im Inland zugeordnet wird. Hierfür ist es notwendig, die entsprechende Kommunikation zu lesen und allenfalls mit weiteren Angaben, welche die Einordnung der Person als inländische erlaubt, zu kombinieren. Eine anonymisierte Weiterleitung erscheint zudem als ungenügender Schutz der Grundrechte der Person, deren Namen anonymisiert worden ist, denn es werden damit gleichwohl sie betreffende Informationen über Kommunikation bzw. Kommunikationsinhalte verwendet. Ausserdem wird es je nachdem, welche Informationen weitergeleitet werden, unschwer möglich sein, die Identität dieser Person trotz der Anonymisierung zu einem späteren Zeitpunkt wieder zu eruieren, sei es über den Inhalt der Kommunikation, über Metadaten oder über die Identität der Kommunikationspartner. Darüber hinaus erlaubt Art. 42 Abs. 3 NDG dem durchführende Dienst die unveränderte Weiterleitung der Daten an den NDB, wenn die Daten Informationen über Vorgänge im In- oder Ausland enthalten, die auf eine konkrete Bedrohung der inneren Sicherheit nach Art. 6 Absatz 1 lit. a NDG hinweisen. Die Verwendung «inländischer» Kommunikation, welche von der Funk- und Kabelaufklärung erfasst ist, ist also im Ergebnis durch das NDG nicht gesamthaft ausgeschlossen. Diese Problematik bestand im Übrigen bereits unter der bisherigen gesetzlichen Grundlage; sie ist mit dem NDB nicht wirksam behoben worden, sondern besteht im Wesentlichen unverändert fort (vgl. insb. GPDel-Bericht vom 9. November 2007, Ziff. 5.2).

13. Die Bestimmung, Angaben über schweizerische natürliche oder juristische Personen seien als Suchbegriffe nicht zulässig, ist als Schranke gegen die Überwachung «inländischer» Personen insoweit kaum wirksam, als sie mit computerlinguistischen Ansätzen umgangen werden kann, indem mit geeigneten Suchbegriffen und deren Auswertung im Ergebnis auf «inländische» Entitäten gezielt werden kann, ohne dass deren Namen oder andere allzu offensichtliche Angaben als Suchbegriff verwendet wird.

14. Bei der Funkaufklärung überlässt es das NDG dem Bundesrat, die Organisation und das Verfahren der Funkaufklärung zu regeln. Auf Gesetzesstufe ist damit kein Verfahren festgelegt, mit dem die Einhaltung der bei der Funkaufklärung zu beachtenden Grundsätze, einschliesslich der Wahrung der Grundrechte, garantiert wäre. Dies weckt Bedenken. Die Organisation und das Verfahren wären hinreichend in einem Gesetz im formellen Sinn festzulegen. Auf diese Weise könnte der Gesetzgeber hinreichend Gewähr dafür bieten, dass ein Genehmigungsverfahren besteht, in dem die Grundrechte ausreichend zum Tragen kommen. In Bezug auf die Funkaufklärung ist dies nicht der Fall.

15. Bei der Kabelaufklärung ist ein Genehmigungsverfahren vorgesehen, bei dem für einen Auftrag zur Kabelaufklärung die Genehmigung des Bundesverwaltungsgerichts sowie die Freigabe durch die Vorsteherin oder den Vorsteher des VBS einzuholen ist (Art. 40 NDG). Im Antrag sind die in Art. 41 NDG vorgesehenen Angaben zu machen.

16. Allerdings kann der Auftrag mit diesen Angaben nicht zureichend und wirksam eingegrenzt werden und lässt sich durch das Bundesverwaltungsgericht nicht hinlänglich überprüfen. So sind im Antrag nicht etwa die Suchbegriffe selbst zu nennen, sondern lediglich die Kategorien von Suchbegriffen. Dies erschwert oder verunmöglicht es dem Bundesverwaltungsgericht, die Folgen des Auftrags für den überwachten Datenverkehr und die daran beteiligten Personen abzuschätzen. Selbst wenn es für das Bundesverwaltungsgericht in einem konkreten Fall einigermassen deutlich würde, wonach gesucht wird, liegen dem Bundesverwaltungsgericht zwar die im Gesuch zu machenden Angaben vor, aber das Gericht weiss damit nicht (und kann nicht wissen), welche Hits die damit verbundenen Suchbegriffe produzieren wird und welche Daten bzw. Personen davon wie betroffen sein werden. Ein Genehmigungsverfahren kann nicht besser sein als das damit verbundene Prüfungsprogramm. Jenseits der Reichweite des richterlichen Prüfprogramms kann ein Gericht nicht beschränkend wirken. Mangels Kenntnis der Details und Hintergründe und weil es die Auswirkungen eines Auftrags bei dessen Überprüfung letztlich nicht kennt und nur sehr beschränkt überprüfen kann, wird das Gericht wesentliche Aspekte eines Auftrags letztlich nicht einschätzen können. Es wird im Wesentlichen nur überprüfen können, ob der Antrag die formellen Voraussetzungen erfüllt, also die im Gesetz verlangten Angaben geliefert werden. Die Stichhaltigkeit der im Antrag gelieferten Angaben, namentlich der

Begründung der Notwendigkeit des Einsatzes, wird sie aber letztlich nicht effektiv überprüfen können.

17. Damit gilt für das gerichtliche Bewillungsverfahren bei der Kabelaufklärung absehbar, was das Office of the United Nations High Commissioner for Human Rights im Bericht vom Juni 2014 festhält, nämlich dass eine gerichtliche Überprüfung nicht als Wundermittel betrachtet werden könne; in mehreren Ländern sei die gerichtliche Überprüfung von digitalen Überwachungsmassnahmen von Geheimdiensten und/oder Strafverfolgungsbehörden zu einer Durchwink-Übung verkommen (A/HRC/27/37, § 38.; http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc):

> *«Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires. At the same time, judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. [...]»*

18. Mit vergleichbaren Problemen wie die gerichtliche Aufsicht sind auch die Aufsichts- und Kontrollorgane konfrontiert (Art. 75 ff. NDG). Diese Organe können ebenfalls nicht abschätzen, welche Hits ein Suchauftrag generieren wird, wessen Kommunikation betroffen sein wird und ob die betroffenen Personen effektiv einen konkreten Anlass gesetzt haben, aufgrund dessen sie richtigerweise in den Fokus des NDB kommen. Die Tätigkeit der Aufsichts- und Kontrollorgane ist insoweit unvermeidlich ineffektiv. Die Problematik der fehlenden Effizienz interner Aufsichtsorgane hat auch das Office of the United Nations High Commissioner for Human Rights, welches im Bericht vom Juni 2014 festhält (A/HRC/27/37, § 37.; http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc):

> *«Article 17, paragraph 2 of the International Covenant on Civil and Political Rights states that everyone has the right to the protection of the law against unlawful or arbitrary interference or attacks. The "protection of the law" must be given life through effective procedural safeguards, including effective, adequately resourced institutional arrangements. It is clear, however, that a lack of*

effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law.»

19. Funkaufklärung wird namentlich über das Projekt Onyx betrieben, einem Projekt zur Aufklärung von Satellitenkommunikationen. Das Projekt Onyx ist von der GPDel untersucht worden im Rahmen der von ihr im Auftrag der Eidgenössischen Räte ausgeübten Oberaufsicht über die Tätigkeit des Bundes im Bereich des Staatsschutzes und der Nachrichtendienste. In den entsprechenden Berichten der GPDel vom 10. November 2003 und vom 9. November 2007 werden einige Aspekte dieses Aufklärungssystems beleuchtet, teilweise unter Bezugnahme auf Erkenntnisse über Kommunikationsabhörsysteme anderer Länder. Im GPDel-Bericht vom 10. November 2003 finden sich Ausführungen zur damaligen Praxis, insbesondere dazu, wie die Suchaufträge und die Schlüsselwörter festgelegt wurden. Die einzelnen Aufklärungsaufträge wurden in Form schriftlicher Leistungsvereinbarungen festgelegt. Die Leistungsvereinbarungen würden sämtliche zur Ausführung und Kontrolle der Aufträge erforderlichen Elemente enthalten, namentlich die gesuchten Aufklärungsobjekte (Namen von Personen, Organisationen oder Unternehmen, Adressteile usw.) sowie die Liste der Schlüsselwörter (Key Words), von denen der Auftraggeber erwartet, dass sie in den abgehörten Kommunikationen erschienen. All diese Informationen seien zur Ausarbeitung automatischer Filtersysteme für die Kommunikationen notwendig. Je nach Auftrag könnten zwischen fünf und mehrere hundert Schlüsselwörter eingegeben werden. Im Bereich der Bekämpfung der Proliferation beispielsweise zähle die Liste der Schlüsselwörter mehr als zehn Seiten mit 25 Begriffen pro Seite. Damals bestanden rund dreissig Leistungsvereinbarungen zwischen dem SND und der EKF und eine Leistungsvereinbarung zwischen dem DAP und der Untergruppe Führungsunterstützung des Generalstabs (GPDel-Bericht vom 10. November 2003, Ziff. 4.5).

20. Die GPDel vertrat im Bericht vom 10. November 2003 auch die Auffasung, dass das gesetzgeberische Dispositiv auf Gesetzesstufe geklärt und präziser gefasst werden müsste, m.a.W. als ungenügend erschien. Die GPGel kritisierte, dass die betroffenen Personen im Ausland im Falle von Abhörungen nicht in den Genuss des Rechtsschutzes des schweizerischen Rechts kämen. Sodann führte sie aus, Artikel 8 EMRK lasse Eingriffe in die Privatleben nur dann zu, wenn es darum gehe, die nationale Sicherheit zu

wahren, und wenn dabei bestimmte Bedingungen wie Bestehen und Zugänglichkeit der rechtlichen Grundlage, Verhältnismässigkeit usw. erfüllt würden. Der EGMR habe in mehreren Entscheiden darauf hingewiesen, dass die Gesetze zur Reglementierung administrativer oder gerichtlicher Abhörungen der Öffentlichkeit zugänglich und ausreichend genau und ausführlich abgefasst sein müssten, so dass die Bürger darauf mit einem adäquaten Verhalten reagieren können. Die GPDel empfahlt vor diesem Hintergrund eine präzisere gesetzliche Grundlage (GPDel-Bericht vom 10. November 2003, Ziff. 5.1.1). Im Bericht vom 9. November 2007 musste die GPDel konstatieren, dass das ihr Anliegen, die Übereinstimmung der Rechtsgrundlagen von Onyx mit der EMRK zu verbessern, bei den seitherigen Revisionen auf Verordnungsstufe nicht berücksichtigt worden war, dies trotz des zwischenzeitlich eingeholten Gutachtens des Bundesamts für Justiz (BJ) vom 31. August 2004, welches ebenfalls grundrechtliche Mängel festgestellt hatte (GPDel-Bericht vom 9. November 2007, Ziff. 5.3). Das Fazit der GPDel gilt, insbesondere was das Erfordernis der Vorhersehbarkeit betrifft, nach Inkrafttreten des NDG unverändert weiter. Von Seiten des Bundesrats ist diese Problematik im gesetzgeberischen Prozess, welcher zum NDG geführt hat, unter den Tisch gekehrt worden. In der Botschaft zum NDG wird ausgeführt, zur Verwendung von Suchwörtern bestehe bereits eine eingespielte, rechtlich korrekte und kontrollierte Praxis aus der Funkaufklärung (Bericht zum Vorentwurf des NDG vom 8. März 2013, S. 51). Dass die GPDel wesentliche Aspekte der Praxis der Funkaufklärung als nicht grundrechtskonform und damit eben rechtlich gerade nicht als korrekt erachtet hat, wird hierbei unterschlagen.

21. Die gesetzliche Grundlage, welche das NDG insb. für die Kabelaufklärung schafft, ist zwar neu. Vergleichbare Systeme sind aber verschiedentlich Gegenstand von Medienberichten, Untersuchungen und Gerichtsentscheiden gewesen, welche sich mit staatlichen Kommunikationsabhörsystemen befasst haben. Erhellend war dabei insbesondere die Auswertung von Erkenntnissen, die sich aus der Snowden-Affäre ergeben haben.

22. Vor diesem Hintergrund wird deutlich, dass mit der Funk- und Kabelaufklärung der insbesondere von der NSA und ihren Partnerorganisationen betriebene Ansatz, möglichst alle erfassbare Kommunikation zu erfassen und computergestützt zu durchsuchen, im kleineren Schweizer Rahmen übernommen werden soll (wobei die Überwachungstätigkeit der Schweizer Behörden in die internationale Zusammenarbeit und den internationalen Datenaustausch der Nachrichtendienste verschiedener Länder eingebettet werden kann).

23. Mit den heutigen Möglichkeiten der Datenverarbeitung kann ein weit mächtigeres System betrieben werden als noch im GPDel-Bericht vom 10. November 2003 beschrieben. Mit dem heutigen Stand der Technik und der jetzigen gesetzlichen Grundlage können viel mehr Datenleitungen

bzw. -ströme gescannt und viel mehr Daten verarbeitet werden, und es stehen leistungsfähigere Computer und ausgeklügeltere Technologien zur Verfügung. Die Snowden-Affäre und ihre Aufarbeitung haben hier einige Erkenntnisse zu Tage gefördert. Einen Einblick, wozu Systeme für die Kabelaufklärung mittlerweilen fähig sind, gewährt der Bericht des NSA-Untersuchungsausschusses von 2017 (Bericht des 1. Untersuchungsausschusses der 18. Wahlperiode des Deutschen Bundestages). Im Rahmen der Operation EIKONAL hat die NSA dem Deutschen Bundesnachrichtendienst «mehrere hunderttausend Selektoren» zum Zweck des Ausspionierens zugeleitet (S. 1355). Es wurde eine «Anlasslose Massenüberwachung in gigantischem Ausmass» festgestellt (S. 1354). Es ist davon auszugehen, dass die Zahl der Aufträge und der Suchbegriffe im Rahmen der Funk- und Kabelaufklärung auch in der Schweiz eine ganz andere Dimension erreicht als noch von der GPDel beschrieben. Die internationale Zusammenarbeit und der Datenaustausch zwischen den Nachrichtendiensten werden das ihre dazu beitragen, die Praxis der Funk- und Kabelaufklärung zu befeuern. Zu erwähnen sind in diesem Zusammenhang Recherchen der «Schweiz am Sonntag» und von ZDF-«Zoom», wonach die NSA hat mit der Schweiz eine geheime Vereinbarung abgeschlossen hat, welche die NSA berechtigt, eigene Schlüsselbegriffe auch in das Abhörsystem der Schweiz einspeisen zu lassen. (https://www.schweizamwochenende.ch/aktuell/geheimdienst-aufsicht-will-kooperation-des-ndb-mit-der-nsa-pruefen-131052001).

24. Dieser Ansatz wird bereits in den erwähnten Berichten der GPDel so beschrieben, einschliesslich der inhärenten Problematik, dass die verschiedenen parallel laufenden Suchaufträge rasch zu einer sehr grossen Zahl von Schlüsselwörtern führen, dass solche Systeme eine Massenüberwachung von Kommunikationen führen und dass die Wirksamkeit und Effektivität solcher Systeme nicht nachgewiesen ist (vgl. GPDel-Bericht vom 10. November 2003, Ziff. 1, Ziff. 4.5, GPDel-Bericht vom 9. November 2007, Ziff. 7.3, Empfehlung 2). Bei den vom DAP erteilten Suchaufträge wurde festgestellt, dass der Prozentsatz der Informationen mit einem Bezug zu schweizerischen Kommunikationsteilnehmern bei 15 % lag (GPDel-Bericht vom 10. November 2003, Ziff. 5.1.3). Die GPDel wies auf Abhörstatistiken des deutschen BND und der amerikanischen NSA hin (GPDel-Bericht vom 10. November 2003, Ziff. 4.6):

> *«Abhörmöglichkeiten des deutschen BND: Von den rund 10 Millionen alltäglich aus und nach Deutschland getätigten internationalen Kommunikationsverbindungen wickeln sich rund 800 000 oder 8 % über Satelliten ab. Knapp 10 % davon (75 000 Kommunikationen) werden durch eine Suchmaschine gefiltert. Es scheint, dass von diesen Gesprächen nur etwa 700 Informationen beinhalten, die möglicherweise Anhaltspunkte für eine*

> *Gefährdung der nationalen Sicherheit enthalten, und dass von diesen 700 höchstens 15 Gegenstand einer eingehenden Überprüfung sein können. Das Verhältnis liegt demnach bei 15 auf 10 Millionen oder 0,00015%.»*
>
> *«Die amerikanische NSA empfängt gemäss Bamford jede Halbstunde eine Million Satellitengespräche. Von dieser Million Kommunikationen würden 6500 durch Filtrierung ausgesondert, 1000 Eingaben entsprächen den vordefinierten Kriterien, 10 würden von Analytikern ausgewählt, und auf dieser Grundlage würde schliesslich ein Bericht ausgefertigt. Hier liegt das Verhältnis bei 1 auf 1 Million, d.h. 0,0001%.»*

25. Eine neuere Untersuchung kommt zum Ergebnis, dass sich gerade einmal 0.26% der beim BND anfallenden Hits als nachrichtendienstlich relevant erwiesen haben https://netzpolitik.org/2016/strategische-ueberwachung-gerade-mal-026-prozent-nachrichtendienstrechtlich-relevant/). Aus allen verfügbaren Untersuchungen wird jedenfalls eine riesige Diskrepanz zwischen der grossen Masse der erfassten Kommunikation und der im Vergleich dazu sehr geringen Zahl der relevanten Hits sichtbar.

26. Gemäss NDG werden die herausgefilterten Daten, die bei der automatisierten Durchforstung der Datenströme nach Suchbegriffen als Hits erscheinen, vom ZEO aufbereitet und aufbewahrt und gegebenenfalls an den NDB weitergeleitet, welcher diese auswertet und weiterverwendet (vgl. insb. Art. 39 NDG und Art. 26 ff. NDV). Die heute vorhandenen Mittel der Datenverarbeitung mit Technologien wie Computerlinguistik, Big Data und Machine Learning erlauben dabei eine sehr ausgeklügelte Suche in den durchlaufenden Datenströmen (vgl. Hernâni Marques Madeira, Massenüberwachung mittels Computerlinguistik und Sprachtechnologie im Lichte der Snowden-Enthüllungen, Zürich 2015 [https://blog.fdik.org/2015-12/masterarbeit--clmassenueberwachung_v1.11_web.pdf]).

27. Allerdings wissen weder der NDB noch das ZEO zum Vornherein, wer zu welchem Zweck über die erfassten Datenströme kommuniziert. Die Funk- und Kabelaufklärung stellen lediglich eine computergestützte Interpretation des Inhalts der Datenströme dar. Es wird versucht, mit den gesetzten Suchbegriffen und den zur Verfügung stehenden Möglichkeiten der Datenbearbeitung relevante Daten herauszufiltern und ihnen damit eine konkrete Bedeutung zu geben. Der Ansatz der Funk- und Kabelaufklärung ist damit notgedrungen ziemlich unspezifisch. Funk- und Kabelaufklärung zielt nicht oder zumindest nicht ausschliesslich und spezifisch auf bestimmte Personen, gegenüber denen der Verdacht einschlägiger Betätigung besteht, sondern stellt eine Methode dar, bei der

mittels Stichworten und Algorithmen versucht wird, für den NDB relevante Kommunikation zu eruieren. Da man nicht im Voraus weiss, wer zu welchem Zweck kommuniziert, ist die Interpretation ausserordentlich schwierig, deutlich schwieriger etwa als im kommerziellen Bereich, wo Anbieter wie Google und Facebook die ihnen zur Verfügung stehenden Daten mittels Analysen und der Verwendung von Big-Data-Ansätzen auswerten. Im kommerziellen Bereich werden vor allen Dingen Daten von eigenen Kunden verwendet, die schon gewisse Angaben hinterlegt haben, oder die zumindest durch die Verwendung von Cookies und anderen Tracking-Methoden als Nutzer individualisiert werden können. Und währenddem Nutzer im kommerziellen Bereich ihre Angaben und Absichten für gewöhnlich offen legen oder zumindest nicht absichtlich verbergen, werden die Personen, für deren Kommunikation sich der NDB interessiert, tendenziell so kommunizieren, dass ihre Identität und ihre Absicht möglichst verborgen bleiben. Es ist deutlich schwerer einzuordnen und abzuschätzen, wie beispielsweise potenzielle Terroristen kommunizieren und was gegebenenfalls ihre Pläne sind bzw. ob es sich überhaupt um potenzielle Terroristen handelt, als etwa das Verhalten eines gewöhnlichen Facebook-Kunden zu interpretieren. Damit ist der mit der Funk- und Kabelaufklärung verbundenen Ansatz, möglichst viele Daten zu erfassen und anhand von Suchbegriffen zu durchsuchen, ohne im Vornherein zu wissen, wer weswegen kommuniziert, mit sehr grossen Schwierigkeiten konfrontiert. Bezeichnet man die relevanten Daten in Analogie zur Signaltechnik als Signale und die irrelevanten als Rauschen, so besteht die Herausforderung darin, die Messung richtig einzustellen, so dass Signale möglichst zuverlässig erfasst wird, aber möglichst wenig Rauschen entsteht. Wird zu wenig gemessen, werden Signale nicht erfasst, wird der Filter zu weit eingestellt, so wird viel Rauschen mit erfasst. Zu viel Rauschen bedeutet, dass Signale u.U. gar nicht erkannt werden. Vor allen Dingen bedeutet Rauschen im konkreten Kontext aber auch, dass Personen bzw. die Kommunikation von Personen in den Fokus des NDB geraten, welche nicht dem Aufgabenbereich des NDB zuzuordnen sind (vgl. Marques Madeira, op. cit.; und die nachstehend, Ziff. II.F.1., zitierten Darlegungen von Bruce Schneier).

28. Im Ergebnis ist zu konstatieren: Funk- und Kabelaufklärung erfasst ganze Datenströme und damit die Kommunikation sehr vieler unbescholtener Personen, indem Kommunikation breit abgeschöpft und nach Stichworten durchsucht wird. Auch allfällige Hits beziehen sich nicht zwingend auf die Kommunikation von Personen, deren Tätigkeit in den Fokus des NDB gehört, sondern können sich ebenso auf vollkommen unbescholtene Personen beziehen. Die Hits resultieren aus der computergestützten Interpretation von Kommunikation, deren Bewandtnis weder der Computer noch die die Hits interpretierenden Mitarbeiter des NDB und ZEO kennen. Auch mit der weiteren Bearbeitung der betreffenden Daten wird es sehr oft kaum möglich sein, die Kommunikation unbescholtener Personen von relevanter Kommunikation zu unterscheiden. In der erhobenen Datenfülle werden also zwangsläufig Daten unbescholtener

Personen erhoben und bearbeitet werden. Es ist gewollter und notwendiger Bestandteil der Funk- und Kabelaufklärung, Kommunikation auch von unbescholtenen Personen zu durchsuchen und auch Hits zu erhalten, die aus der Kommunikation von unbescholtenen Personen stammt, ohne dass diese sofort wieder ausgeschieden werden könnten. Mit dieser Überwachungsmethode wird damit bewusst in Kauf genommen, auch vollkommen unbescholtene Personen zu überwachen.

29. Die Funk- und Kabelaufklärung stellen somit eine anlasslose Massenüberwachung dar. Die Überwachung besteht in einer ersten Stufe darin, dass alle erfassten Datenströme und damit die Kommunikation aller Personen, welche Bestandteil dieser Datenströme ist, nach Suchbegriffen durchforstet werden. Findet sich in den Datenströmen ein Hit, so führt dies zu weiteren Stufen von Überwachung. Über den ganzen Prozess hinweg wird nicht nur die Kommunikation von Personen überwacht, welche der NDB anhand seines Aufgabenbereichs (Art. 6 NDG) in den Fokus nehmen darf, sondern – entsprechend dem Ansatz einer Rasterfahndung – auch die Kommunikation sehr vieler weiterer Personen. Die im Gesetz vorgesehenen Instrumente, mit welchen diese Überwachung eingedämmt werden sollen, wirken wie dargelegt nicht oder nur ungenügend.

30. Werden Daten vom NDB ausgewertet und weiterverwendet, so werden die Daten gespeichert, mit Interpretationen versehen, mit weiteren Daten kombiniert und allenfalls an weitere Stellen im In- und Ausland weitergegeben. Diese weitere Datenverarbeitung und -weitergabe setzt voraus, dass sie einem im NDG vorgesehenen Zweck (Art. 2 NDG) entspricht und einer im NDG vorgesehenen Aufgabe (Art. 6 NDG) dient (vgl. auch Art. 25 NDV) . Somit wird mit der weiteren Datenverarbeitung und -weitergabe zumindest die Vermutung verbunden sein, von den Kommunikationspartnern gehe eine der in Art. 6 Abs. 1 NDG bzw. Art. 25 NDV genannten Bedrohungen der inneren oder äusseren Sicherheit aus. Aufgrund dieser Etikettierung können sie Ziel weiter Überwachungs- oder Zwangs- und Verwaltungsmassnahmen von Seiten in- oder ausländischer Nachrichtendienste, Strafverfolgungsbehörden und weiteren Behörden werden. Dazu ist festzustellen, dass diese Etikettierung naturgemäss sehr oft nicht mehr als eine Vermutung sein wird; der Umgang mit ungesicherten Informationen und das Bestreben, Informationen zu erlangen, oft bei ungesicherter Faktenlage, sind essenzieller Bestandteil nachrichtendienstlicher Tätigkeit.

C. Tangierte Grundrechte

1. Die Funk- und Kabelaufklärung greift in verschiedene Grundrechte ein. Sie ist damit nur rechtmässig, wenn sie sich über eine genügende gesetzliche Grundlage verfügt, sich auf ein öffentliches Interesse stützen kann und verhältnismässig ist, sie muss also geeignet und erforderlich sein, um den beabsichtigten Zweck zu erreichen, und das öffentliche Interesse muss gegenüber den Interessen der betroffenen Person überwiegen (Art. 36

BV). Die Rechtfertigung eines Eingriffs in Art. 8 EMRK setzt voraus, dass der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Die Freiheit auf Meinungsäusserung nach Art. 10 EMRK kann Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung.

2. Die Funk- und Kabelaufklärung tangiert das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]). Diese Normen verleihen jeder Person das Recht, frei von staatlicher Überwachung mit anderen Personen zu kommunizieren. Dies betrifft jede Form von Kommunikation, unabhängig davon, wo und mit welchen Mitteln die Kommunikation geführt wird. Geschützt ist sowohl der Inhalt der Kommunikation als auch die Tatsache an sich, dass die Kommunikation stattfindet, namentlich Ort und Zeit der Kommunikation sowie die Identität der daran teilnehmenden Personen. Diese Grundrechte sind damit immer dann tangiert, wenn der Staat Daten im Zusammenhang mit der Kommunikation von Personen erfasst, durchsucht und speichert, und zwar sowohl in Bezug auf den Inhalt der Daten als in Bezug auf sogenannte Metadaten. Der schwere Eingriff liegt bereits in der Erfassung der Daten und der damit verbundenen Überwachung an sich (vgl. JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, S. 203 ff.,).

3. Die Funk- und Kabelaufklärung tangiert weiter die Freiheit der Meinungsäusserung, die Meinungs- und Informations- sowie die Medienfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II) und die Versammlungsfreiheit (Art. 22 BV, Art. 11 EMRK). Diese Normen verleihen jeder Person das Recht, ihre Meinung frei von staatlichen Eingriffen zu bilden und zu äussern, Medien und weitere Informationsquellen selbst und frei von staatlichen Eingriffen zu konsultieren, ihre Meinung mit anderen Menschen auszutauschen und sich friedlich mit anderen Personen zu versammeln (vgl. MÜLLER/SCHEFER, a.a.O., S. 347 ff., S. 437 ff., S. 517 ff., S. 571 ff.). Im Zusammenhang mit Art. 19 UNO-Pakt II ist hervorgehoben worden, dass dieser Artikel zwischen Meinung und Meinungsbildung

einerseits und Meinungsäusserung andererseits differenziert. Art. 19 UNO-Pakt II erlaubt unter gewissen Voraussetzungen Einschränkungen der Meinungssäusserung, nicht aber des Rechts, eine Meinung zu haben, und es wird deutlich gemacht, was die Meinungsfreiheit im digitalen Zeitalter beinhaltet. So schreibt David Kaye, Special Rapporteur of the Human Rights Council, in seinem Report on the promotion and protection of the right to freedom of opinion and expression vom Mai 2015 (A/HRC/29/32; http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc):

> *«19. The first article of the Universal Declaration of Human Rights recognizes that everyone is "endowed with reason and conscience", a principle developed further in human rights law to include, among other things, the protection of opinion, expression, belief, and thought. Article 19 (1) of the International Covenant on Civil and Political Rights, also echoing the Universal Declaration, provides that "everyone shall have the right to hold opinions without interference". Opinion and expression are closely related to one another, as restrictions on the right to receive information and ideas may interfere with the ability to hold opinions, and interference with the holding of opinions necessarily restricts the expression of them. However, human rights law has drawn a conceptual distinction between the two. During the negotiations on the drafting of the Covenant, "the freedom to form an opinion and to develop this by way of reasoning was held to be absolute and, in contrast to freedom of expression, not allowed to be restricted by law or other power".[1] The ability to hold an opinion freely was seen to be a fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction. Consequently, the permissible limitations in article 19 (3) expressly apply only to the right to freedom of expression in article 19 (2). Interference with the right to hold opinions is, by contrast, per se in violation of article 19 (1).*
>
> *20. Commentators and courts have devoted much less attention to the right to hold opinions than to expression. Greater attention is warranted, however, as the mechanics of holding opinions have evolved in the digital age and exposed individuals to significant vulnerabilities. Individuals regularly hold opinions digitally, saving their views and their search and*

browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. In other words, holding opinions in the digital age is not an abstract concept limited to what may be in one's mind. And yet, today, holding opinions in digital space is under attack. [...]

21. The right to hold opinions without interference also includes the right to form opinions. Surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes. [...]»

4. Sodann sind die persönliche Freiheit und die Bewegungsfreiheit garantiert (Art. 10 Abs. 2 BV, Art. 8 EMRK). Diese Grundrechte schützen das Recht, die Persönlichkeit frei von staatlichen Eingriffen zu entfalten, die wesentlichen Aspekte seines Lebens selber zu gestalten, persönliche Beziehungen zu knüpfen, allein gelassen zu werden und sich frei zu bewegen (vgl. MÜLLER/SCHEFER, a.a.O., S., 139 ff., S. 83 ff.).

5. Die Überwachungsmassnahmen betreffen auch die Kommunikation zwischen den GesuchstellerInnen und allfälligen BerufsgeheimnisträgerInnen i.S.v. Art. 321 StGB (insb. Geistliche, RechtsanwältInnen und ÄrztInnen). Es bestehen keine rechtlichen oder tatsächlichen Vorkehren, welche garantieren würden, dass Kommunikation mit Berufsgeheimnisträgern nicht von der Kabel- und Funkaufklärung erfasst und als Folge davon ausgewertet und vom NDB verwendet werden. Wenn die GesuchstellerInnen BerufsgeheimnisträgerInnen konsultieren, ist die Kommunikation mit diesen, soweit sie elektronisch erfolgt, nicht von der Funk- und Kabelaufklärung ausgenommen und insofern nicht vor Überwachung geschützt. Sie müssen damit rechnen, dass auch ihre Kommunikation mit Geheimnisträgern von der Funk- und Kabelaufklärung erfasst wird, dass sie also auch bezüglich solcher Kommunikation überwacht werden. Das Vertrauensverhältnis zwischen den GesuchstellerInnen und Geheimnisträgern wird dadurch erschüttert. Darin liegt ein spezifischer und schwer wiegender Eingriff in das Recht der GesuchstellerInnen auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (MÜLLER/SCHEFER, a.a.O., S. 214 m.w.H.).

6. Schliesslich ist Unschuldsvermutung tangiert (Art. 6 EMRK, Art. 32 BV). Jeder Mensch gilt als unschuldig, so lange er nicht in einem rechtmässig geführten Verfahren für schuldig befunden wurde, einen gesetzlich umschriebenen Tatbestand erfüllt zu haben. Eine angeschuldigte Person hat das Recht auf Aussageverweigerung, sie muss sich nicht selbst belasten (nemo-tenetur-Grundsatz). Die Unschuldsvermutung ist auch im Rahmen des Datenschutzes zu beachten (vgl. MÜLLER/SCHEFER, a.a.O., S. 981 ff.).

7. Die GesuchstellerInnen 4, 5 und 6 sind als JournalistInnen tätig und deshalb von der Funk- und Kabelaufklärung speziell betroffen. Sie sind für die Ausübung ihres Berufes verstärkt darauf angewiesen, frei von Überwachung und unter Wahrung des Quellenschutzes recherchieren und andere Personen kontaktieren zu können. Wird ihre Kommunikation von der Funk- und Kabelaufklärung erfasst und analysiert, so können daraus Rückschlüsse auf ihre beruflichen Aktivitäten, ihre Recherchen und ihre Kontakte zu Drittpersonen gezogen werden. Namentlich sind mit den gespeicherten Daten Schlüsse auf Kontakte mit journalistischen Quellen und deren Angaben möglich. Die vorstehend dargelegten Grundrechtseingriffe wirken damit bei JournalistInnen noch verstärkt. Dies gilt namentlich auch für die Intransparenz und mangelnde Vorhersehbarkeit, die mit der Funk- und Kabelaufklärung verbunden ist, und dem mit der vagen gesetzlichen Grundlage verbundenen «chilling effect» (dazu MÜLLER/SCHEFER, a.a.O., S. 377). Art. 17 BV garantiert die Medienfreiheit. Gestützt auf Art. 17 Abs. 3 BV und Art. 10 EMRK anerkennen der EGMR und das Bundesgericht den Schutz journalistischer Quellen als eine der Grundbedingungen der Medienfreiheit. Eine Pflicht zur Preisgabe der anvertrauten Informationen könnte die Informanten abschrecken. Die Praxis des EGMR stützt sich dabei auf die Freiheit der Meinungsäusserung, die Praxis des Bundesgerichts überdies auf das Redaktionsgeheimnis. Geschützt ist namentlich die Identität des Autors sowie Inhalt und Quelle der Information. Medienschaffende können ihre Aufgabe als Informationsvermittler und Wächter nur erfüllen, wenn sie die erforderliche Information von Dritten erhalten, insbesondere Hinweise auf Vorkommnisse von gesellschaftlichem Interesse, die sonst verborgen bleiben würden. Dies wiederum setzt voraus, dass die Informationsgeber darauf vertrauen können, dass ihr Name nicht preisgegeben wird. Eine Pflicht zur Preisgabe der anvertrauten Informationen könnte Informanten abschrecken («chilling effect»). Unter Schutz steht damit insbesondere die Identität der Quelle. Gemäss Strassburger Praxis vermögen nur zwingende Gründe des öffentlichen Interesses die Aufhebung des Redaktionsgeheimnisses zu rechtfertigen. Es ist jedenfalls ein überwiegendes öffentliches Interesse erforderlich. Nach der Praxis des Bundesgerichts bedarf die Offenbarungspflicht ausserordentlicher Umstände (MÜLLER/SCHEFER [mit FRANZ ZELLER], a.a.O., S. 472; FROWEIN/PEUKERT, EMRK-Kommentar, 3. Aufl., Kehl am Rhein 2009, Art. 10 Rn. 17; JENS MEYER-LADEWIG, Handkommentar EMRK, 3. Aufl., Baden-Baden 2011, Art. 10 Rn. 39; Basler-Komm/ZELLER, Art. 172 StPO, N 2, N 7

f.; DONATSCH, in: Kommentar zur Schweizerischen Strafprozessordnung, DONATSCH/HANSJAKOB/LIEBER (Hrsg.), 2. Aufl., Zürich/Basel/Genf 2014, Art. 172 N 2 und N 4; Basler-Komm/BOMMER/GOLDSCHMID, Art. 264 StPO, N 15; VIKTOR GYÖRFFY, Quellenschutz im Strafprozess, in: medialex 6/16 sowie medialex Jahrbuch 2016, S. 79 ff., Rz. 2 f.; EGMR, 27.3.1996, Goodwin v. The United Kingdom (GC), 17488/90; EGMR, 22.11.2007, Voskuil v. The Netherlands, 64752/01; BGE 132 I 184; BGE 140 IV 108).

8. Der Gesuchsteller 8 ist als Rechtsanwalt tätig. Wie vorstehend (Ziff. 5.) dargelegt bestehen keine rechtlichen oder tatsächlichen Vorkehren, welche garantieren würden, dass Kommunikation mit Berufsgeheimnisträgern nicht von der Kabel- und Funkaufklärung erfasst und als Folge davon ausgewertet und vom NDB verwendet werden. Wenn der Gesuchsteller 8 mit seinen Klienten kommuniziert, ist diese Kommunikation, soweit sie elektronisch erfolgt, nicht von der Funk- und Kabelaufklärung ausgenommen und insofern nicht vor Überwachung geschützt. Er und seine Klienten müssen damit rechnen, dass auch die Kommunikation zwischen ihnen von der Funk- und Kabelaufklärung erfasst wird, dass sie also auch bezüglich solcher Kommunikation überwacht werden. Das Vertrauensverhältnis zwischen dem Gesuchsteller 8 und seinen Klienten wird dadurch erschüttert. Dies stellt einen Eingriff in das Recht der Gesuchsteller auf Achtung des Privatlebens und auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung. Ebenfalls tangiert ist die Wirtschaftsfreiheit (Art. 27) des Gesuchstellers 8, da dieser Eingriff den Gesuchsteller 8 in seiner wirtschaftlichen Tätigkeit tangiert. Der grundrechtliche Schutz muss bei Trägern von Berufsgeheimnissen besonders intensiv sein. Das hier massgebliche Vertrauensverhältnis verdient Vorrang und muss unangetastet bleiben. Die Überwachung von Anschlüssen von Geheimnisträger wie Anwälten ist nur erlaubt, wenn gegen den Betroffenen Anwalt selber ein dringender Tatverdacht besteht, oder wenn konkrete Anhaltspunkte vorliegen, dass sein Telefonanschluss für kriminelle Zwecke verwendet wird (MÜLLER/SCHEFER, a.a.O., S. 191 und S. 214 f. m.w.H.).

9. Ein Aspekt des Grundrechtseingriffs liegt darin, dass die Funk- und Kabelaufklärung einen «chilling effect» auf das Kommunikations- und Informationsverhalten hat. Wer damit rechnen muss, dass er überwacht wird, wenn er kommunizieren und sich informieren will, wird tendenziell weniger von seinen Möglichkeiten, über elektronische Kanäle zu kommunizieren und sich zu informieren, weniger Gebrauch machen. Seine Kommunikationsmöglichkeiten und seine Möglichkeit, eine Meinung zu bilden, sind dadurch eingeschränkt. Auch in diesem abschreckenden Effekt liegt ein Grundrechtseingriff. Ein «chilling effect» kann auch aus einer vagen gesetzliche Grundlage resultieren, die den rechtsanwendenden Behörden einen derart grossen Spielraum lässt, dass für die Einzelnen die rechtlichen Konsequenzen einer Meinungsäusserung kaum abschätzbar

sind. Deshalb ist aus dem Gedanken des grundrechtlichen Schutzes freier Kommunikation und der Gefahr unerwünschter «chilling effects» an die Bestimmtheit der gesetzlichen Grundlage von Grundrechtseingriffen besonders strenge Anforderungen zu stellen (MÜLLER/SCHEFER, a.a.O., S. 375 ff.). Wie an anderer Stelle dargelegt (Ziff. II.D.) ist die gesetzliche Grundlage für die Funk- und Kabelaufklärung zu unbestimmt, was wesentlich zu diesen abschreckenden Effekten beiträgt.

10. Die GesuchstellerInnen nutzen verschiedene elektronische Kommunikationsmittel, insbesondere Telefon, Internet (namentlich WWW), E-Mail und andere Messenger-Dienste. Dabei kommunizieren sie von der Schweiz aus, teilweise vom Ausland, mit anderen Personen und Gegenstellen im In- und Ausland. Der dabei anfallende Datenverkehr läuft mindestens teilweise über Kommunikationskanäle, namentlich Satelliten und Glasfaserleitungen, deren Datenströme von der Funk- und Kabelaufklärung erfasst werden können bzw. erfasst werden. Aufgrund des Aufbaus der Kommunikationsstrukturen ist kaum absehbar, über welche Kommunikationskanäle die konkrete Kommunikation läuft. Die GesuchstellerInnen müssen somit zumindest damit rechnen, dass ihre Kommunikation von der Funk- und Kabelaufklärung erfasst und nach Suchbegriffen durchsucht wird. Sie müssen auch damit rechnen, dass sich aus dieser Durchsuchung Hits in ihrer Kommunikation finden, die dazu führen, dass ihre Kommunikation vom ZEO erfasst, aufbereitet und aufbewahrt und gegebenenfalls an den NDB weitergeleitet wird, welcher diese auswertet und weiterverwendet.

11. Die Funk- und Kabelaufklärung besteht wie dargelegt (II.B.) darin, dass grosse Datenströme computergestützt ausgewertet und interpretiert werden, ohne dass der NDB weiss, wer hier aus welchem Grund kommuniziert. Den über diese Datenströme kommunizierenden Personen ist nicht klar, dass ihre Kommunikation durchforstet wird und was konkret zu Hits führt. Aufgrund dieser Natur der Funk- und Kabelaufklärung ist für die GesuchstellerInnen nicht vorhersehbar, ob und in welchem Fall ihre Kommunikation Gegenstand der Funk- oder Kabelaufklärung wird und allenfalls zu Hits führt. Sie können ihre gewohnte Kommunikation auf elektronischem Weg nicht durchführen, ohne zu riskieren, in den Fokus der Funk- oder Kabelaufklärung zu gelangen. Ihre Kommunikation ist insoweit Gegenstand einer Massenüberwachung. Ihre in der Kommunikation enthaltenen Daten und allenfalls weitere Daten können, wenn die Kommunikation zu Hits führt, Gegenstand konkreter Auswertungen und weiterer Datenverarbeitung durch den NDB und allenfalls weiterer in- und ausländischer Behörden werden. Die GesuchstellerInnen erfahren nichts davon, wenn ihre Kommunikation gegebenenfalls Gegenstand der Funk- und Kabelaufklärung ist, da diese Massnahme heimlich durchgeführt wird.

12. Die Beurteilung, die in verschiedenen Berichten Office of the United Nations High Commissioner for Human Rights allgemein zu staatlichen

Überwachungsmassnahmen getroffen wird, trifft auch auf die Funk- und Kabelaufklärung zu. So stellt Joe Cannataci, Special Rapporteur on the right to privacy, in seinem Report on the right to privacy vom Oktober 2016 eine steigende Tendenz von Regierungen fest, einschneidendere Überwachungsmassnahmen zu propagieren, welche zu einer kaum verhüllten Massenüberwachung führen (A/71/368, https://www.privacyandpersonality.org/wp-content/uploads/2016/10/cb_ref_1_10_oct_2016.docx). Solche Massenüberwachungen führen zu übermässigen und nicht zu rechtfertigenden Eingriffen. Sie erscheinen als willkürlich, selbst wenn sie einem legitimen Zweck dienen und sich auf eine gesetzliche Grundlage stützen. Es genügt nicht, dass Massnahmen darauf abzielen, Nadeln im Heuhaufen zu finden, Massnahmen sind vielmehr daran zu messen, welche Auswirkungen sie auf den Heuhaufen haben (Report oft he Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age (A/HRC/27/37, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc) vom Juni 2014, § 25). Betont wird auch die Klarheit, Bestimmtheit und die Vorhersehbarkeit als Voraussetzung für Überwachungsmassnahmen (Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedomof opinion and expression, im Report vom April 2013 (A/HRC/23/40, § 83; http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf) fest

13. Der Eingriff in die genannten Grundrechte, insbesondere in das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung und in das Recht auf Meinungsfreiheit, liegt bereits insofern vor, als dem NDB mit der Funk- und Kabelaufklärung die Möglichkeit eingeräumt wird, Datenströme auszuleiten und zu analysieren, in denen Kommunikation der GesuchstellerInnen enthalten sein kann. Gemäss der Praxis des EGMR beinhaltet bereits die blosse Existenz einer Gesetzgebung, welche ein System zur heimlichen Überwachung von Kommunikation erlaubt, die Gefahr einer Überwachung all derer, auf die die Gesetzgebung angewendet werden könnte. Diese Bedrohung tangiert unvermeidlich die Freiheit der Kommunikation zwischen Benutzern der Telekommunikationsservices und führt damit zu einem Eingriff in Art. 8 EMRK, unbesehen der Massnahmen, die effektiv gegen die Betroffenen geführt werden (vgl. Liberty and Others v. The United Kingdom [58243/00], EGMR, 12. Juli 2008, § 56; Weber and Saravia v. Germany [54934/00], EGMR, 29. Juni 2006, § 78; GPDel-Bericht vom 10. November 2003, Ziff. 5.1.1 m.w.H. in Fn 42). Der Eingriff beginnt somit damit, dass das NDG dem NDB die Durchführung der Funk- und Kabelaufklärung erlaubt, und setzt sich fort und wird zunehmend konkreter, soweit effektiv Kommunikation der GesuchstellerInnen in

ausgeleiteten Datenströmen erfasst wird, diese Kommunikation allenfalls zu Hits führt und die Kommunikation allenfalls weiter vom NDB analysiert und mit anderen Daten verbunden und gespeichert wird.

14. Über die dargelegten Aspekte hinaus sind die Gesuchsteller von der Funk- und Kabelaufklärung konkret wie folgt betroffen:

15. Die Gesuchstellerin 1 ist in ihrer eingangs erwähnten Tätigkeit als gemeinnütziger Verein betroffen (vgl. Ziff. I.7.). Sie ist in dieser Tätigkeit darauf angewiesen, sich zu den von ihr bearbeiteten Themen frei informieren zu können, ungehindert Informationen zur Verfügung stellen zu können und ohne staatliche Überwachung mit Mitgliedern, weiteren interessierten Personen und anderen Organisationen im In- und Ausland kommunizieren zu können.

16. Der Gesuchsteller 2 lebt in der Schweiz. Er kommuniziert sowohl geschäftlich als auch im Rahmen seines ehrenamtlichen zivilgesellschaftlichen Engagements viel auf elektronischem Weg mit ausländischen Kommunikationspartnern. Die Kommunikationsmassenüberwachung, gegen die sich die vorliegende Beschwerde richtet, ist für ihn in zweierlei Hinsicht schier unerträglich: Einerseits, weil er professionell über Telefon und andere elektronische Kommunikationskanäle Coaching anbietet und die Coachees im Rahmen der Coaching-Gespräche oft auch über sehr persönliche Themen sprechen. Andererseits wegen seines ehrenamtlichen zivilgesellschaftlichen Engagements im Rahmen der Just Net Coalition, die sich im Internet-Kontext für Menschenrechte und soziale Gerechtigkeit einsetzt. In diesem Zusammenhang ist er darauf angewiesen, international mit Human Rights Defenders kommunizieren zu können, ohne befürchten zu müssen, dass diese Kommunikation nachrichtendienstlich überwacht wird und eventuell sogar Informationen über Kommunikationsinhalte an Nachrichtendienste oder sonstiger Behörden anderer Länder weitergegeben werden können.

17. Der Gesuchsteller 3 ist Informatiker und Geschäftsleiter der Digitalen Gesellschaft. In seinen beruflichen Tätigkeiten berät und schult er Unternehmen und Organisationen sowie speziell auch Berufsgeheimnisträger und JournalistInnen im Bereich der sicheren und vertraulichen Kommunikation. Nicht von der systematischen Telekommunikationsüberwachung erfasst zu werden, gestaltet sich jedoch immer schwieriger. Der Grad der staatlichen Überwachung nimmt durch die Kabelaufklärung drastisch zu. Wer nicht in der Lage ist, der Überwachung zu entgehen, wird sein Kommunikationsverhalten und seinen Bewegungsfreiraum einschränken («chilling effect»). Freie Meinungsäusserung, Versammlungsfreiheit, schlussendlich Teilhabe an demokratischen Prozessen sind beeinträchtigt. Genau diese Prinzipien muss eine freiheitliche, demokratischen Gesellschaft jedoch gewährleisten. Dafür stehen unsere verfassungsmässig garantieren Grundrechte ein. Die Funk- und Kabelaufklärung kollidiert fundamental mit diesen

Freiheitsrechten. Der Gesuchsteller 3 passt bereits heute sein Kommunikationsverhalten den Überwachungsmassnahmen an. Die seit 2002 in der Schweiz geltende Vorratsdatenspeicherung legt z.B. eine Verwendung von Diensten im Ausland nahe. Genau diese sind nun von der Funk- und Kabelaufklärung speziell betroffen. Der Gesuchsteller 3 kann die mannigfaltigen Möglichkeiten der elektronischen Kommunikation aufgrund der Überwachungsmassnahmen nur mit gewichtigen Beschränkungen nutzen. Insgesamt wird seine Kommunikation durch die Kabelaufklärung nochmals deutlich weiter eingeschränkt.

18. Die Gesuchstellerin 4 ist freischaffende Journalistin, Ko-Präsidentin des Recherche-Netzwerks investigativ.ch und Mitglied des «International Consortium of Investigative Journalists». Sie ist Beraterin bei Journalismfund.eu und Mitarbeiterin beim «Investigative Reporting Project Italy». Neben ihrer Arbeit als Journalistin unterrichtet sie investigativen Journalismus und betreut StudentInnen. Die Gesuchstellerin 4 arbeitet vorwiegend in internationalen Recherche-Teams und ist darauf angewiesen, dass das Redaktionsgeheimnis gewahrt bleibt. In ihrer journalistischen Tätigkeit teilt die Gesuchstellerin vertrauliche Informationen mit ihren Kontakten per Email und Telefon über internationale Telekommunikationsverbindungen. Sie ist essenziell darauf angewiesen, dass der Schutz ihrer journalistischen Quellen gewährleistet ist. In diesem Zusammenhang ist sie zusätzlich darauf angewiesen, international kommunizieren zu können, ohne befürchten zu müssen, dass diese Kommunikation nachrichtendienstlich überwacht wird und eventuell sogar Informationen über Kommunikationsinhalte an Nachrichtendienste oder sonstige Behörden anderer Länder weitergegeben werden können.

19. Die Gesuchstellerin 5 ist Journalistin bei der Wochenzeitung WOZ. In ihrer journalistischen Tätigkeit teilt die Gesuchstellerin vertrauliche Informationen mit ihren Kontakten per Email und Telefon auch über internationale Telekommunikationsverbindungen. Einer ihrer aktuellen Schwerpunkte betrifft die Fluchtrouten von Afrika nach Europa. Ihre Erlebnisse an Bord des Rettungsschiffes Sea-Watch 2 sind eben als Buch unter dem Titel «Mission Mittelmeer» erschienen. Von der Satellitenaufklärung ist konkret auch der Schiffsfunk und die Kommunikation zum Festland betroffen. So werden über die Satelliten von Inmarsat nicht nur Notsignale und Funksprüche, sondern auch nicht öffentliche Telefonie und Daten ins Internet übertragen. Aus dem Bericht der GPDel vom 10. November 2003 kann geschlossen werden, dass das auf der Sea-Watch 2 verwendete System Eutelsat ebenfalls zu den Abhörzielen des Nachrichtendienstes des Bundes gehört. (http://www.weltwoche.ch/ausgaben/2005_10/artikel/was-sagen-sie-jetzt-die-weltwoche-ausgabe-102005.html). In ihren Recherchen steht die Gesuchstellerin in Kontakt u.a. mit Flüchtlingen, Behörden, Menschenrechtsorganisationen, PolitikerInnen und AnwältInnen, oft also mit Kontakten, die besonders exponiert sind. Sie ist essenziell darauf

angewiesen, dass der Schutz ihrer journalistischen Quellen gewährleistet ist.

20. Der Gesuchsteller 6 ist 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. In seiner journalistischen Tätigkeit teilt der Gesuchsteller 6 vertrauliche Informationen mit seinen Kontakten per Email und Telefon über internationale Telekommunikationsverbindungen. Er arbeitet mit Bürgerrechtsorganisationen in westlichen Demokratien wie auch in repressiven Staaten oder gar Bürgerkriegsregionen zusammen. So hat er z.B. den Aufbau des syrischen Überwachungsstaates und die Verstrickung westlicher Firmen gemeinsam mit Privacy International dokumentiert [https://netzpolitik.org/?p=141138]. Der Gesuchsteller 6 ist oft in Ländern wie Türkei, Russland, Mexiko, Kolumbien, Vietnam oder Myanmar unterwegs, die Ziele von Überwachung sein dürften. 2015 wurde gegen Andre Meister und seine Quelle(n) auf Geheiss des Deutschen Verfassungsschutzes ein Ermittlungsverfahren wegen Landesverrats eröffnet. Er hatte als vertraulich eingestufte Dokumente publiziert, aus denen hervorgeht, dass der Geheimdienst «soziale Medien» wie Twitter oder Facebook stärker überwachen will. Das Verfahren musste später eingestellt werden, zeigt jedoch plastisch, dass der Gesuchsteller 6 durch seine journalistische Tätigkeit besonders exponiert ist. In seiner journalistischen Tätigkeit ist der Gesuchsteller essenziell darauf angewiesen, dass der Schutz seiner journalistischen Quellen gewährleistet ist. Der Gesuchsteller 6 wohnt und arbeitet in Deutschland. Die Funk- und Kabelaufklärung zielt speziell auf den ausländischen und internationalen Datenverkehr. Der Gesuchsteller 6 ist entsprechend von den Überwachungsmassnahmen durch den NDB betroffen. Erschwerend wirkt, dass die mittels der Funkaufklärung empfangenen Informationen auch ein nützliches «Tauschmittel» mit den entsprechenden Dienststellen im Ausland bilden (vgl. GPDel-Bericht vom 10. November 2003, Ziff. 5.3).

21. Der Gesuchsteller 7 ist Politikwissenschaftler und Journalist. Er ist u.a als Redakteur des Bulletins von Solidarité sans frontières (sosf) in Bern tätig. sosf setzt sich ein für die Grundrechte aller Flüchtlinge und MigrantInnen, unabhängig vom Aufenthaltsstatus und engagiert sich für eine offenere Migrationspolitik. Der Gesuchsteller 7 ist zudem als Redaktor der Zeitschrift «Bürgerrechte & Polizei/CILIP» in Berlin tätig, welche sich seit 1978 kritisch mit der Tätigkeit von Polizei und anderen Sicherheitsbehörden befasst. In seiner journalistischen Tätigkeit teilt der Gesuchsteller 7 vertrauliche Informationen mit seinen Kontakten per Email und Telefon über internationale Telekommunikationsverbindungen. Er ist in der Schweiz und in Deutschland als Journalist tätig. Die Funk- und Kabelaufklärung zielt speziell auf den ausländischen und internationalen

Datenverkehr. Der Gesuchsteller 7 ist entsprechend von den Überwachungsmassnahmen durch den NDB betroffen.

22. Der Gesuchsteller 8 ist als Rechtsanwalt vorwiegend in den Bereichen Strafrecht, internationales Strafrecht, internationale Rechtshilfe in Strafsachen, Ausländerrecht und Grundrechte/Europäische Menschenrechtskonvention (EMRK) tätig. In dieser Tätigkeit ist er immer wieder in Fälle involviert, welche rechtspolitisch, politisch und/oder medial besonders exponiert sind, so etwa Fälle, welche politische Verfolgung, die Ahndung von Kriegsverbrechen, die Verantwortung international tätiger Konzerne für Verbrechen oder strafrechtliche Vorwürfe mit Bezug auf Terrorismus und gewalttätigen Extremismus zum Gegenstand haben. Der Gesuchsteller 8 hat dabei auch viele internationale Kontakte mit entsprechender Kommunikation über internationale Telekommunikationsverbindungen, dabei auch mit Menschen, die für ihre politische Tätigkeit von repressiven Staaten verfolgt werden. Für seine Tätigkeit als Rechtsanwalt ist er essenziell darauf angewiesen, kommunizieren zu können, ohne dass er und seine Klienten befürchten müssen, dass ihre Kommunikation und ausgetauschte Daten vom Nachrichtendienst gescannt, bearbeitet und an weitere Dienste und Behörden im In- und Ausland weitergegeben werden.

23. Als Fazit muss festgehalten werden, dass die Gesuchsteller durch die Funk- und Kabelaufklärung schwer wiegende Eingriffe in die vorstehend genannten Grundrechte erleiden.

D. Gesetzliche Grundlage

1. Die Funk- und Kabelaufklärung stützt sich auf die im NDG enthaltene gesetzliche Grundlage (vgl. im Einzelnen vorstehend II.B.).

2. Der bestehenden gesetzlichen Grundlage lässt sich allerdings nicht mit hinreichender Klarheit entnehmen, was Gegenstand der Funk- und Kabelaufklärung ist und wer alles in welcher Art und Weise von diesen Massnahmen betroffen ist. Bei einer Massnahme, die zu schwer wiegenden Grundrechtseingriffen zahlreicher Personen führt, muss für die Betroffenen mit hinreichender Klarheit ersichtlich sein, dass und auf welche Art und Weise ihre Grundrechte tangiert sind. Die Auswirkungen müssen aufgrund des Gesetzes mit hinreichender Klarheit vorhersebar sein. Diese Anforderungen erfüllt die gesetzliche Grundlage der Funk- und Kabelaufklärung nicht.

3. Aus der sehr abstrakten gesetzlichen Umschreibung der Funk- und Kabelaufklärung ist für die Rechtsunterworfenen nicht ersichtlich, dass potenziell die gesamte elektronische Kommunikation Gegenstand der Funk- und Kabelaufklärung ist und wie diese ausgewertet und weiterverwendet werden kann. Obschon eine abstrakte gesetzliche Grundlage besteht, ist für niemanden in genügender Weise vorhersehbar,

unter welchen Umständen seine Kommunikation von der Funk- und Kabelaufklärung erfasst werden kann. Es ist kaum abschätzbar, über welche Kanäle die eigen Kommunikation gehen wird und ob einer dieser Kanäle von der Funk- und Kabelaufklärung erfasst wird. Es ist ebenfalls nicht einzuschätzen, welche Art von Kommunikation, bezogen auf den Inhalt und auf die Metadaten, einen Hit und die weitere Bearbeitung der Daten durch den ZEO und den NDB auslösen können.

4. Es wird hier eine grundsätzliche Problematik der nachrichtendienstlichen Tätigkeit sichtbar. Dieser wohnt eine Heimlichkeit inne, die auch in der Formulierung der gesetzlichen Grundlagen ihren Niederschlag findet. Zwar ist eine solche geschaffen worden. Darin kommt aber zum Ausdruck, dass Überwachungsmöglichkeiten geschaffen werden sollen, bei denen die potenziellen Zielpersonen nicht ermessen können, dass und in wie weit sie davon betroffen sein könnten. Als Folge dieses Ansatzes ist jedoch generell für Rechtsunterworfene kaum zu durchschauen, in wie weit und auf welche Weise ihre Kommunikation von der Funk- und Kabelaufklärung betroffen ist.

5. Da die Funk- und Kabelaufklärung zu schwer wiegenden Eingriffen in Grundrechte führt, muss sie sich auf eine genügend klare gesetzliche Grundlage stützen können. Genügend klar ist die gesetzliche Grundlage, wenn sich aus ihr für die Rechtsunterworfenen mit hinreichender Deutlichkeit ergibt, dass und in wie weit diese von der Funk- und Kabelaufklärung tangiert sind. Deren Auswirkungen müssen aufgrund des Gesetzes hinreichend deutlich vorhersehbar sein. Dies ist bei den konkreten gesetzlichen Bestimmungen nicht der Fall. Die Funk- und Kabelaufklärung verfügt damit nicht über eine genügende gesetzliche Grundlage. In Bezug auf die Eingriffe in Grundrechte, welche von der EMRK geschützt werden, erscheint die Funk- und Kabelaufklärung als ungesetzlich. Sie verletzt damit die Grundrechte der GesuchstellerInnen, insbesondere Art. 8 EMRK.

6. Diese Schlussfolgerung erscheint vor dem Hintergrund der Entscheid der Strassburger Organe unvermeidlich. Gemäss Praxis des EGMR muss das Gesetz, auf welches sich geheime Überwachungsmassnahmen stützt, so hinreichend deutlich sein, dass der Bürger daraus entnehmen kann, unter welchen Voraussetzungen die Behörden solche Massnahmen treffen dürfen. Überwachungsmassnahmen müssen auf einem besonders präzise abgefassten Gesetz fussen. Die Existenz von klaren und ausführlichen Regeln ist in diesem Bereich unabdingbar, um so mehr, als sich die zum Einsatz gelangenden technischen Verfahren immer weiter entwickeln. Der Umfang des den Behörden eingeräumten Ermessensspielraums und die Art seiner Anwendung bei der Überwachung muss gesetzlich klar geregelt sein. Der Fokus der Massnahmen muss im Gesetz hinreichend klar geregelt sein, so dass Personen einen hinreichend klaren Schutz davor erhalten, beliebig oder willkürlich davon betroffen zu sein. Die betroffene Person muss in der Lage sein, die sich aus dem Gesetz ergebenden Konsequenzen

für sich einschätzen zu können (Vorhersehbarkeit). Auch die Bedingungen für die Speicherung müssen mit hinreichender Klarheit festgelegt sein. Ein Überwachungsprogramm zur automatisierten Durchsuchung vieler Telekommunikationsleitungen erfüllt diese Voraussetzungen nicht, auch wenn sich an sich in einem Gesetz vorgesehen sind und die Behörden abstrakt verpflichtet sind, die Grundrechte bei der Durchführung des Programms zu beachten (MEYER-LADEWIG, a.a.O., Art. 8 Rn. 35; FROWEIN/PEUKERT, a.a.O., Art. 8 Rn. 16; Liberty and Others v. The United Kingdom [58243/00], EGMR 12. Juli 2008, §§ 59ff., § 69; Weber and Saravia v. Germany [54934/00], EGMR, 29. Juni 2006, §§ 93 f.; Amann v. Switzerland [27798/95], GC, 16. Februar 2000; GPDel-Bericht vom 10. November 2003, Ziff. 5.1.1 m.w.H. in Fn 42).

7. Im Fall Liberty, welcher sich auf ein entsprechendes Überwachungsprogramm in Grossbritannien bezog, hielt der EGMR fest:

> *«64. The Court recalls that section 3(2) of the 1985 Act allowed the executive an extremely broad discretion in respect of the interception of communications passing between the United Kingdom and an external receiver, namely to intercept "such external communications as are described in the warrant". There was no limit to the type of external communications which could be included in a section 3(2) warrant. According to the applicants, warrants covered very broad classes of communications, for example, "all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe", and all communications falling within the specified category would be physically intercepted (see paragraph 43 above). In their observations to the Court, the Government accepted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication intercepted under a section 3(2) warrant (see paragraph 47 above). The legal discretion granted to the executive for the physical capture of external communications was, therefore, virtually unfettered.*
>
> *65. Moreover, the 1985 Act also conferred a wide discretion on the State authorities as regards which communications, out of the total volume of those physically captured, were listened to or read. At the time of issuing a section 3(2) interception warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted*

material which he considered should be examined. Again, according to the applicants, certificates were formulated in general terms and related only to intelligence tasks and priorities, such as, for example, "national security", "preventing or detecting serious crime" or "safeguarding the economic well-being of the United Kingdom" (see paragraph 43 above). On the face of the 1985 Act, only external communications emanating from a particular address in the United Kingdom could not be included in a certificate for examination unless the Secretary of State considered it necessary for the prevention or detection of acts of terrorism (see paragraphs 23-24 above). Otherwise, the legislation provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy.

66. Under section 6 of the 1985 Act, the Secretary of State, when issuing a warrant for the interception of external communications, was called upon to "make such arrangements as he consider[ed] necessary" to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary. The applicants contend that material was selected for examination by an electronic search engine, and that search terms, falling within the broad categories covered by the certificates, were selected and operated by officials (see paragraph 43 above). According to the Government (see paragraphs 48-51 above), there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that details of these "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.

67. The fact that the Commissioner in his annual reports concluded that the Secretary of State's "arrangements" had been complied with (see paragraphs 32-33 above), while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme,

> *since he was not able to reveal what the "arrangements" were. In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge. [...]*
> *69. In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law".*
> *70. It follows that there has been a violation of Article 8 in this case.»*

8. Auch das Office of the United Nations High Commissioner for Human Rights betont, dass eine genügende gesetzliche Grundlage vorhanden sein muss, wozu gehört, dass die Anwendung des Gesetzes für die Rechtsunterworfenen hinreichend vorhersehbar ist ("The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 vom Juni 2014 [http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc], m.w.H.; vgl. im Weiteren die Ausführungen zur Verhältnismässigkeit, nachstehend II.G.):

> *«28. Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law. "Accessibility" requires not only that the law is published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given action may entail. The State must ensure that any*

interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.
29. […] A law that is accessible, but that does not have foreseeable effects, will not be adequate.»

9. Die gesetzliche Regelung der Funk- und Kabelaufklärung erfüllt die dargelegten Anforderungen an eine gesetzliche Grundlage von Überwachungsmassnahmen eindeutig nicht. Es ist für die betroffenen Personen und damit für die GesuchstellerInnen nicht hinreichend klar, vorhersehbar und nachprüfbar, in welchen Fällen und unter welchen Voraussetzungen sie von der Funk- und Kabelaufklärung erfasst werden und was für Konsequenzen dies für sie hat. Sie sind davor sicher, beliebig oder willkürlich in den Fokus der Funk- und Kabelaufklärung zu geraten. Der gesetzliche Rahmen ist hierfür zu weit und zu unklar. Die GesuchstellerInnen können ihr Verhalten – anders als wenn es etwa um strafbares Verhalten geht – nicht am Gesetz ausrichten. Der Fokus der Funk- und Kabelaufklärung ist derart weit, d.h. er kann sich auf derart verschiedenartiges Kommunikationsverhalten richten, dass nicht abgeschätzt werden kann, was davon erfasst wird und was zu Hits führen könnte. Dies liegt gerade auch an der hierbei computerbasierten, neurolinguistischen Datenverarbeitung unter Verwendung von Konzepten von Big-Data und Machine-Learning. Nicht nur, dass die Suchbegriffe nicht bekannt sind. Zum Vornherein festgelegt werden bei einem Suchauftrag ja Kategorien von Suchbegriffen, die Suchbegriffe werden danach festgelegt und können im Verlauf der Ausführung des Auftrags verändert werden, nicht zuletzt wiederum mit Hilfe von Neurolinguistik und Machine-Learning. Der Verwendung von Big-Data- und Machine-Learning-Konzepten ist inhärent, dass der Datenbearbeitungsprozess nicht nur auf einem ursprünglichen Input basiert, was zu analysieren ist, sondern sich durch die Bearbeitung der Daten laufend verändert und sich vom ursprünglichen Input – konkret von den Suchbegriffen – löst. Damit ist bei der Funk- und Kabelaufklärung schlichtweg für niemand vorhersehbar, was aus der Datenverarbeitung resultieren wird. Es geht ja gerade darum, eine Analyse aus einer grossen Mende von Ergebnisse zu erhalten, welche nur mit Hilfe modernster Computertechnologie zustande gebracht werden kann.

10. Der gesetzlichen Regelung auch griffige Bestimmungen zur akkuraten Beurteilung der Relevanz gewonnener Daten, zur weiteren Verwendung gewonnener Daten, zur Ausscheidung und zu Löschung von Daten. Auch das gesetzlich vorgesehene Auskunftsrecht erscheint als ungenügend. Hierbei darf nicht übersehen werden, dass die aus der Funk- und Kabelaufklärung gewonnenen Daten ihrer Natur nach bezüglich ihrer Bedeutung, Relevanz und persönlicher Zuordnung regelmässig kaum akkurat einzuordnen sein werden. Bei einer computerbasierten Datenverarbeitung unter Verwendung von Konzepten von Big-Data und Machine-Learning wird für den Anwender selbst oft kaum nachvollziehbar sein, nach welcher Logik die Datenverarbeitung genau vorgeht (gerade auf dieser verselbständigten Bearbeitung beruhen diese Konzepte). Bestehende Bestimmungen zur Datenbearbeitung können damit in Bezug auf die Datenbearbeitung im Rahmen der Funk- und Kabelaufklärung nur sehr beschränkt Wirkung entfalten.

11. Insgesamt fehlt es der Funk- und Kabelaufklärung damit an einer hinreichend klaren und bestimmten gesetzlichen Grundlage. Die GesuchstellerInnen können wie vorstehend dargelegt nicht hinreichend abschätzen und abschätzen, was die Funk- und Kabelaufklärung für sie bedeutet. Sie sind damit in ihren Grundrechten verletzt, soweit diese tangiert sind.

E. Öffentliches Interesse

1. Das öffentliche Interesse besteht in den im NDG, insbesondere im Zweckartikel (Art. 2 NDG) genannten wichtigen Landesinteressen sowie den Bereichen, die im Zusammenhang mit den Aufgaben des NDG genannt werden (Art. 6 NDG), deren Schutz die Funk- und Kabelaufklärung zu dienen hat. Das öffentliche Interesse besteht damit vor allen Dingen in der Wahrung der öffentlichen Sicherheit, wobei der Begriff der wichtigen Landesinteressen darüber hinaus geht und auch eine wirtschaftliche Komponente aufweisen kann, was u.a. aus Art. 6 Abs. 1 lit. a al. 4 NDG deutlich wird, welcher sich auf kritische Infrastrukturen bezieht, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind.

2. Die Funkaufklärung dient gemäss Art. 38 Abs. 2 NDG der Beschaffung sicherheitspolitisch bedeutsamer Informationen über Vorgänge im Ausland, insbesondere aus den Bereichen Terrorismus, Weiterverbreitung von Massenvernichtungswaffen und ausländische Konflikte mit Auswirkungen auf die Schweiz sowie der Wahrung weiterer wichtiger Landesinteressen nach Art. 3 NDG.

3. Die Kabelaufklärung kann zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland (Art. 6 Abs. 1 Bst. b NDG) sowie zur Wahrung weiterer wichtiger Landesinteressen nach Art. 3

durchgeführt werden. Der Zweck der Funkaufklärung ist in Art. 25 NDV festgelegt.

4. Die Funk- und Kabelaufklärung hat damit grundsätzlich wichtigen Landesinteressen zu dienen. Der Begriff der wichtigen Landesinteressen ist allerdings sehr weit und aus sich heraus kaum einzugrenzen, und den konkret genannten Zwecken und Aufgabenbereichen kann höchst unterschiedliches Gewicht zukommen.

5. Hinzu kommt, dass die Bedrohungen der genannten öffentlichen Interessen, die es durch die Tätigkeit des NDG abzuwehren gilt, oft vage und schwer zu erfassen ist. Das zeigt gerade die Funk- und Kabelaufklärung. Anders als in einem Strafverfahren, für dessen Eröffnung ein Verdacht auf ein konkretes Delikt vorliegen muss und bei dem sich Zwangsmassnahmen gegen Personen richten, die konkret der Begehung einer Straftat verdächtigt werden, richtet sich die Funk- und Kabelaufklärung gerade nicht gegen eine konkrete Person aufgrund eines konkreten Verdachts. Die Funk- und Kabelaufklärung dient vielmehr dazu, durch eine computergestützte Rasterfahndung in Datenströmen Kenntnisse zu erlangen. Die Faktenlage, welche zur Anordnung eine Funk- oder Kabelaufklärung führt, ist notgedrungen wenig konkret, andernfalls bedürfte es dieser Massnahme gar nicht. Bei der Gewichtung des öffentlichen Interesses ist somit zu berücksichtigen, dass die Ausgangslage bei der Anordnung der Massnahme sehr viel unspezifischer ist als etwa bei der polizeilichen Gefahrenabwehr oder bei Zwangsmassnahmen im Strafprozess.

F. Eignung und Erforderlichkeit

1. Wie dargelegt, besteht der Ansatz der Funk- und Kabelaufklärung darin, breit Datenströme zu erfassen und computergestützt zu analysieren, um so Daten herauszufiltern, welche für den NDB relevant sind. Der Nutzen dieses Ansatzes für nachrichtendienstliche Tätigkeiten muss sehr in Frage gestellt werden. Be der Festlegung der Suchwörter und der durchsuchten Datenströme ist nicht bekannt, wer konkret mit welchem Inhalt über diese Datenleitungen kommunizieren wird und in wie weit und mit welchen Inhalten dabei Personen kommunizieren, welche für den Nachrichtendienst von Belang sind. Die Erteilung eines entsprechenden Suchauftrags dient ja gerade dem Ziel, mit Datenerfassung und -analyse Erkenntnisse zu gewinnen. Wie dargelegt ist es im nachrichtendienstlichen Bereich das Problem, bei den durchforsteten Daten relevante von irrelevanten Kommunikationen zu unterscheiden, äusserst gross. Bruce Schneier, weltweit anerkannter Experte für Kryptographie und Computersicherheit, hat sich eingehend mit dieser Problematik befasst und hat überzeugend dargelegt, dass solche Formen von Massenüberwachung, wie sie die Funk- und Kabelaufklärung darstellen, Terrorismus nicht eindämmen und verhindern können (BRUCE SCHNEIER, Data and Goliath, The Hidden Battles to Collect Your Data and Control Your World; in deutscher Übersetzung:

Data und Goliath - Die Schlacht um die Kontrolle unserer Welt, New York/London, 2015; http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist). Data Mining könne erfolgreich sein, um Werbung zu platzieren. Es funktioniere am besten, wenn nach bekannten Profilen gesucht wird, wenn es genügend Ereignisse gibt, anhand deren Suchprofile optimiert werden können und wenn die Folgen eines falschen Alarms nicht gravierend sind. Das Erkennen von Kreditkartenbetrug sei ein Beispiel, wo Data Mining gut funktioniert. Um Terroristen aufzuspüren müssten die Angaben dagegen viel akkurater sein, als es Data-mining Systeme zu liefern vermöchten. Entsprechende Ereignisse seien vergleichsweise selten, womit selbst akkurate Systeme zur Vorhersage von Terrorismus derart von falschen Alarmen überflutet würden, dass sie nutzlos wären. Die in diesem Zusammenhang insbesondere aus US-amerikanischen Geheimdienstkreisen zu hörende Überlegung, um eine Nadel im Heuhaufen zu finden, brauche es einen Heuhaufen zeigt aus Sicht von Bruce Schneier gerade das Problem. Was jemand, der eine Nadel suche, zuletzt wolle, sei, noch viel mehr Heu auf den Haufen zu werfen. Es sei wissenschaftlich nicht zu halten, anzunehmen, durch das Hinzufügen irrelevanter Daten über unschuldige Personen werde es einfacher, einen terroristischen Angriff zu entdecken. Man mag dadurch etwas mehr Signal erhalten, aber man fügt vor allen Dingen mehr Rauschen zu. In militärischen Geheimdienstkreisen werde das Problem mit «Trinken aus einem Feuerwehrschlauch» («drinking from a fire hose») umschrieben: so viel irrelevante Daten zu haben, dass es unmöglich ist, die wichtigen Datenstücke zu finden. Ein weiteres Problem liege darin, dass jede Terror-Attacke einmalig sei. Es ist damit schwierig, im Vornherein Muster festzulegen, nach denen zu suchen ist. Die Personen, nach denen gesucht werde, würden zudem trickreich agieren und versuchen zu vermeiden, dass sie entdeckt werden. Hier liegt ein entscheidender Unterschied zum personalisierten Marketing, wo die typische Zielperson nicht versucht, ihre Aktivitäten zu verstecken. Ein feindseliges Verhältnis zu einer potenziellen Zielperson verstärkt das Problem ungemein, was dazu führt, dass gängige Big-Data-Analysetools schlichtweg nicht funktionieren können. Bruce Schneier spricht der Massenüberwachung gekoppelt mit Data Mining die Eignung, Terrorismus zu verhindern, deshalb insgesamt ab, und ist der Auffassung, die Kosten hierfür seien nicht zu rechtfertigen. Massenüberwachung sei mitnichten effizienter als herkömmliche nachrichtendienstliche Tätigkeit. Bruce Schneier erachtet es deshalb als kontraproduktiv, Mittel für derartige geheimdienstliche Massenüberwachung einzusetzen, welche dann für andere nachrichtendienstliche Tätigkeiten fehlen.

2. Der Special Rapporteur on the right to privacy,Joseph A. Cannataci, äussert sich in seinem Report on the right to privacy, vom Februar 2017 (A/HRC/34/60, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx) ebenfalls sehr kritisch zur Wirksamkeit und Verhältnismässigkeit von Massenüberwachungen. Symbolpolitik und

eine Psychologie der Angst seien als Rechtfertigung für Eingriffe in Menschenrechte untauglich:

> *«42 [...] a. [...] 2015-2017 have seen a growing tendency, especially though not exclusively in Europe, to indulge in "gesture-politics". In other words, the past eighteen months have seen politicians who wish to be seen to be doing something about security, legislating privacy-intrusive powers into being – or legalise existing practices – without in any way demonstrating that this is either a proportionate or indeed an effective way to tackle terrorism.*
> *b. The new laws introduced are predicated on the psychology of fear: the disproportionate though understandable fear that electorates may have in the face of the threat of terrorism. The level of the fear prevents the electorate from objectively assessing the effectiveness of the privacy-intrusive measures proposed.*
> *c. There is little or no evidence to persuade the SRP of either the efficacy or the proportionality of some of the extremely privacy-intrusive measures that have been introduced by new surveillance laws in France, Germany, the UK and the USA. Like Judge Robart in the recent case on the immigration ban in the USA, the SRP must seek evidence for the proportionality of the measures provided for by laws. In the same way as Judge Robart asked as to precisely how many cases of terrorism were carried out since 2001 by nationals of the states subjected to the immigration ban, the SRP must ask as to whether it would not be much more proportional, never mind more cost-effective and less privacy-intrusive if more money was spent on the human resources required to carry out targeted surveillance and infiltration and if less effort were expended on electronic surveillance. This, in a time when the vast majority of all terrorist attacks were carried out by suspects already known to the authorities prior to the attacks.»*

3. Das Office of the United Nations High Commissioner for Human Rights hebt in seinem Report on the right to privacy in the digital age (A/HRC/27/37, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc) vom Juni 2014 hervor, dass die Beweislast für die Wirksamkeit bei den Behörden liegt:

> *«23. [...] Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim.»*

4. Wie an anderer Stelle dargelegt haben Untersuchungen gezeigt, dass eine riesige Diskrepanz zwischen der grossen Masse der erfassten Kommunikation und der im Vergleich dazu sehr geringen Zahl der relevanten Hits besteht (Ziff. II.B.24. ff.). Auch dies spricht klar gegen die Effizienz dieses Massenüberwachungsansatzes.

5. Die Eignung und Erforderlichkeit der Funk- und Kabelaufklärung zur Erreichung der genannten öffentlichen Interessen ist damit nicht gegeben. An der Eignung bestehen grösste Zweifel, da die massenhafte computergestützte Auswertung von Datenströmen für die Erkennung von Aktivitäten, welche für den NDB relevant sind, als ungeeignet erscheint. Diese Form von Massenüberwachung ist nicht effektiv. Da es andere Formen von staatlichem Vorgehen gegen die einschlägigen Bedrohungen gibt, welche wirksam erscheinen, insbesondere nachrichtendienstliches und strafrechtliches, kann nicht gesagt werden, die Funk- und Kabelaufklärung sei zur Wahrung der öffentlichen Interessen erforderlich. Die Funk- und Kabelaufklärung stellt vielmehr eine Fehlallokation von staatlichen Ressourcen dar.

G. Verhältnismässigkeit und Grundrechtskonformität

1. Die Funk- und Kabelaufklärung ist wie dargelegt mit schweren Eingriffen in die Grundrechte der GesuchstellerInnen verbunden. Diese können verbreitete elektronische Kommunikations- und Informationskanäle nicht mehr nutzen, ohne damit rechnen zu müssen, dass der NDB die Kommunikation abzweigt, um sie zu analysieren und allenfalls weiter zu verwenden. Sie können nicht wissen, ob ihre Kommunikation Gegenstand der Funk- und Kabelaufklärung ist und gegebenenfalls weiter verwendet und an andere Stellen im In- und Ausland weitergegeben wird. Die GesuchstellerInnen sind dadurch stark in ihren Grundrechten tangiert.

2. Das mit der Funk- und Kabelaufklärung verbundene öffentliche Interesse wiegt nicht schwer. Wohl wird die Wahrung gewichtiger öffentlicher Interessen anvisiert. Das Mittel der Funk- und Kabelaufklärung vermag zur Wahrung dieser Interessen jedoch kaum etwas zu leisten, da es ein sehr unspezifisches Vorgehen darstellt, an dessen Eignung grosse Zweifel bestehen und welches nicht als erforderlich erscheint.

3. In der Güterabwägung ist überdies zu berücksichtigen, dass mit der Funk- und Kabelaufklärung eine Massenüberwachung ermöglicht werden soll,

welche potenziell auf alle Personen zielt, deren Kommunikation über die überwachbaren Datenströme geht und dass bei der Erfassung und Auswertung der Datenströme keine Gewähr dafür besteht, dass nur Personen erfasst werden, deren Aktivitäten nachrichtendienstlich relevant sind. Es handelt sich also um ein Konzept, welches nicht im Ansatz auf die Kommunikation einschlägig tätiger Personen beschränkt bleiben kann, sondern notwendigerweise die massenhafte Überwachung unbescholtener Personen beinhaltet.

4. Dieser Ansatz wird vom Office of the United Nations High Commissioner for Human Rights in mehreren Berichten als unzulässig betrachtet, insbesondere mit Blick auf die Verhältnismässigkeit. Joe Cannataci, Special Rapporteur on the right to privacy, schreibt in seinem Report on the right to privacy vom Oktober 2016 (A/71/368, https://www.privacyandpersonality.org/wp-content/uploads/2016/10/cb_ref_1_10_oct_2016.docx):

> *«28. Despite the rulings of numerous national constitutional and regional human rights courts, the Special Rapporteur observes that there is an increased tendency for governments to promote more invasive laws for surveillance, which allow for the thinly disguised permanent mass surveillance of citizens.»*

Der Special Rapporteur on the promotion and protection of the right to freedomof opinion and expression, Frank La Rue, halt in seinem Report vom April 2013 (A/HRC/23/40, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf) fest:

> *«81. Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances [...]»*
>
> *83. Legal frameworks must ensure that communications surveillance measures:*
> *(a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;*
> *(b) Are strictly and demonstrably necessary to achieve a legitimate aim; and*

> *(c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.*

Noch deutlicher wird das Office of the United Nations High Commissioner for Human Rights in seinem Report on the right to privacy in the digital age (A/HRC/27/37, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc) vom Juni 2014, m.w.H.:

> *«21. Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant". In other words, interference that is permissible under national law may nonetheless be "unlawful" if that national law*
> *is in conflict with the provisions of the International Covenant on Civil and Political Rights. The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances". The Committee interpreted the concept of reasonableness to indicate that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".*
> *[...]»*

> *«23. [...] Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim.»*

> *«24. Governments frequently justify digital communications surveillance programmes on the*

grounds of national security, including the risks posed by terrorism. [...] Surveillance on the grounds of
national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.»

«25. [...] Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.»

5. Es besteht kein überwiegendes Interesse, welches diese massenhafte und undifferenzierte Überwachung unbescholtener Personen zu rechtfertigen vermag. Das Interesse an der Wahrung der Grundrechte all dieser unbescholtenen Personen überwiegt klar. Insbesondere haben die GesuchstellerInnen, die selbst keinen Anlass gesetzt haben, Ziel einer nachrichtendienstlichen Überwachung zu sein, ein überwiegendes Interesse daran, dass ihre Grundrechte nicht von der Funk- und Kabelaufklärung tangiert werden. Die Funk- und Kabelaufklärung ist damit nicht verhältnismässig und erscheint nicht als gerechtfertigt.

H. Journalistischer Quellenschutz

1. Das NDG enthält keinerlei Vorkehren, um journalistische Quellen zu schützen. Die Funk- und Kabelaufklärung analysiert jegliche Kommunikation, welche in den erfassten Datenströmen enthalten ist. Damit wird unvermeidlich auch allfällige Kommunikation im erfassten Datenstrom zwischen JournalistInnen und ihren Quellen analysiert. Ein konkreter Anlass, geschweige denn ein genügender Grund, um die Kommunikation zwischen Journalist und Quelle zu erfassen, besteht nicht. Wird die Kommunikation zwischen Journalist und Quelle so gescannt, so ist der Anspruch auf Quellenschutz bereits verletzt; die Überwachung der geschützten Kommunikation ist Tatsache. Führt die Kommunikation zu einem Hit und werden die entsprechenden Daten in der Folge weiterverarbeitet, vertieft sich diese Verletzung des Anspruchs. Sollten der ZEO oder der NDB hierbei von sich aus die Daten aussondern und nicht weiterbearbeiten, weil sie feststellen, dass es sich um Kommunikation

zwischen Journalist und Quelle handelt, ändert das an der Verletzung des Anspruchs nichts. Erstens ist diese bereits eingetreten. Zweitens gehört es u.a. gerade zum Anspruch auf Quellenschutz, dass nicht bekannt wird, dass eine Person journalistische Quelle ist. Die Aussonderung der Daten müsste damit zwangsläufig auf einer Information beruhen, die es gerade zu schützen gilt. In aller Regel werden der ZEO und der NDB ohnehin nicht erkennen können, dass es sich um zu schützende Kommunikation zwischen Journalist und Quelle handelt. Im Übrigen ist nicht vorgesehen, dass Daten, die dem journalistischen Quellenschutz unterliegen, auszusondern sind und nicht bearbeitet werden dürfen. So oder so sind JournalistInnen und ihre Quelle nicht sicher davor, dass ihre Kommunikation vom NDB gescannt und danach weiterbearbeitet wird.

2. Damit müssen JournalistInnen und ihre Quellen damit rechnen, dass ihre Kommunikation Gegenstand einer Überwachung wird, wenn sie dafür weit verbreitete elektronische Kommunikationskanäle benutzen. Sie können nicht darauf vertrauen, dass Schweizer Behörden den ihnen zustehenden Anspruch auf journalistischen Quellenschutz achten. Dies ist geeignet, JournalistInnen in ihren Kontakten zu Quellen zu hemmen, und potenzielle journalistische Quellen könnten dadurch davon abgehalten werden, mit ihnen in Kontakt zu treten. Hierdurch ist der Anspruch auf Quellenschutz verletzt.

3. Dies betrifft konkret insbesondere die GesuchstellerInnen 4, 5 und 6, welche journalistisch tätig sind. Sie werden in ihrem Anspruch auf Quellenschutz verletzt.

I. Berufsgeheimnisse, insb. Anwaltsgeheimnis

1. Das NDG sieht auch keinen wirksamen Schutz von Berufsgeheimnissen vor. Ebenso wie beim journalistischen Quellenschutz ist festzustellen, dass die Funk- und Kabelaufklärung jegliche Kommunikation anlasslos analysiert, welche in den erfassten Datenströmen enthalten ist, und damit unvermeidlich auch allfällige Kommunikation zwischen einem Berufsgeheimnisträger und Personen, die diesen konsultieren. Der Anspruch auf Schutz des Berufsgeheimnisses wird dadurch verletzt. Sollten der ZEO oder der NDB bei einer weiteren Verwendung von Daten feststellen, dass diese dem Berufsgeheimnis unterliegen und die Daten aussondern und nicht mehr verwenden, so macht dies die Verletzung nicht rückgängig. Einen wirksamen Schutz gegen die weitere Verwendung solcher Daten gibt es nicht. In aller Regel werden der ZEO und der NDB ohnehin nicht erkennen können, dass es sich um Kommunikation handelt, welche durch das Berufsgeheimnis geschützt ist.

2. Dies beeinträchtigt Berufsgeheimnisträger in ihrer beruflichen Tätigkeit, und es tangiert generell die Kommunikation zwischen Berufsgeheimnisträgern und Personen, welche sie konsultieren, über verbreitete elektronische Kanäle. Berufsgeheimnisträger und Personen,

welche sie konsultieren oder konsultieren wollen, können nicht darauf vertrauen, dass Schweizer Behörden das Berufsgeheimnis achten. Kommunikation zwischen Berufsgeheimnisträgern und Personen, welche sie konsultieren (möchten), wird dadurch ungerechtfertigt erschwert oder verunmöglicht.

3. Die GesuchstellerInnen sind dadurch in ihrem Anspruch, frei von Überwachung bzw. ohne dass der Staat hiervon irgend etwas erfährt, mit Berufsgeheimnisträgern zu kommunizieren, und somit in ihrem Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung verletzt.

4. Der Gesuchsteller 8 ist als Rechtsanwalt in seinem Anspruch, frei von Überwachung bzw. ohne dass der Staat hiervon irgend etwas erfährt, mit bestehenden und potenziellen Klienten zu kommunizieren, und somit in seinem Recht auf Achtung des Privatlebens und in seiner Wirtschaftsfreiheit verletzt.

J. Verwendung in Strafverfahren und Unschuldsvermutung

1. Das NDG sieht vor, dass nachrichtendienstlich gewonnene Erkenntnisse, insbesondere solche aus der Funk- und Kabelaufklärung, in Strafverfahren und zur Aufrechterhaltung der öffentlichen Ordnung verwendet werden: Dienen Erkenntnisse des NDB anderen Behörden zur Strafverfolgung, zur Verhinderung von schweren Straftaten oder zur Aufrechterhaltung der öffentlichen Ordnung, so stellt der NDB ihnen diese unter Wahrung des Quellenschutzes unaufgefordert oder auf Anfrage hin zur Verfügung (Art. 60 Abs. 2 NDG). Dies ist unvereinbar mit einer Reihe von strafprozessualen Grundsätzen. Die in der StPO enthaltenen Garantien, welche insbesondere ein rechtsstaatlich einwandfreies Vorgehen der Strafverfolgungsbehörden und das rechtliche Gehör der beschuldigten Person sicherstellen sollen, können so im Zusammenspielt zwischen NDB und Strafverfolgungsbehörden ausgehebelt werden. Nachdem grundsätzlich keine Einsicht in Akten des NDB möglich ist und der Schutz nachrichtendienstlicher Quellen im NDG verabsolutiert ist, wird das behördliche Vorgehen, welches zur Einleitung des Strafverfahrens führt, kaum nachvollziehbar sein, soweit auf vom NDB stammende Informationen abgestellt wird. Der Schutz nachrichtendienstlicher Quellen wird dazu führen, dass der tatsächliche Ursprung eines Tatverdachts verschleiert wird. Es dürften sich dazu jeweils keine oder nur nebulöse Hinweise in den Akten finden (*«Polizeiliche Ermittlungen haben ergeben…»*). Insbesondere im Drogenbereich besteht offenbar eine international gängige Praxis der Strafverfolgungsbehörden, den effektiven Ursprung des Tatverdachts zu verschleiern, insbesondere, wenn er auf nachrichtendienstliche Informationen zurückgeht, etwa durch die Inszenierung von scheinbar zufälligen Polizeikontrollen (vgl. http://www.

reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805, wo ein Beamter der amerikanischen Drug Enforcement Administration [DEA] zu diesem als *«parallel construction»* bezeichneten Ansatz wie folgt zitiert wird: *«Parallel construction is a law enforcement technique we use every day, It's decades old, a bedrock concept.»*). Solchem Vorgehen öffnet das NDG Tür und Tor. Die Verfahrensrechte der beschuldigten Person bleiben dabei auf der Strecke. Der rechtsstaatliche Grundsatz, dass Zwangsmassnahmen nur ergriffen werden können, wenn ein hinreichender Tatverdacht vorliegt (vgl. NIKLAUS OBERHOLZER, Grundzüge des Strafprozessrechts, 3. Aufl., Bern 2012, S. 310, Rz. 848), wird verletzt. All dies gilt gerade auch für die Funk- und Kabelaufklärung, bei der eine anlasslose Massenüberwachung dazu führen kann, dass eine Person in ein Strafverfahren verwickelt wir, und dies, ohne das die strafprozessualen Garantien und das rechtliche Gehör der betroffenen Person in Bezug auf die nachrichtendienstliche Basis der Belastung zum Tragen kommen. Das sich Art. 60 Abs. 2 auf schwere Straftaten bezieht, ändert an diesem Befund nichts.

2. Diese Verwischung der Grenzen zwischen Strafverfolgung und Nachrichtendienst ist auch vom Office of the United Nations High Commissioner for Human Rights kritisiert worden, so im Report on the right to privacy in the digital age (A/HRC/27/37, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc) vom Juni 2014:

> *«27. One factor that must be considered in determining proportionality is what is done with bulk data and who may have access to them once collected. Many national frameworks lack "use limitations", instead allowing the collection of data for one legitimate aim, but subsequent use for others. The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resulting sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another. [...]»*

Und der Special Rapporteur on the promotion and protection of the right to freedomof opinion and expression, Frank La Rue, im Report vom April 2013 (A/HRC/23/40, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf) gibt zu bedenken:

> *«79. States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.»*

3. Der Umstand, dass zahlreiche Personen überwacht werden, ohne dass sie einen konkreten Anlass dafür gegeben haben, und als Folge dieser Überwachung negative Folgen gewärtigen müssen, stellt auch eine Verletzung der Unschuldsvermutung dar, zumal die gewonnenen Daten u.U. ungeprüft und ohne dass die Betroffenen involviert gewesen sind, an andere Stellen gelangen können mit unabsehbaren Folgen.

K. Wahrung der Grundrechte für in- und ausländische Bevölkerung, Schutz vor Diskriminierung

1. Der Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 vom Juni 2014 (m.w.H.) (http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc) weist darauf hin, dass ein Staat seinen völkerrechtlichen Verpflichtungen zur Wahrung der Menschenrechte nicht entgehen durch Handlungen ausserhalb seines Territoriums entgehen kann.

> *«33. The Human Rights Committee has been guided by the principle, as expressed even in its earliest jurisprudence, that a State may not avoid its international human rights obligations by taking action*
> *outside its territory that it would be prohibited from taking "at home". This position is consonant with the views of the International Court of Justice, which has affirmed that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State "in the exercise of its jurisdiction outside its own territory", as well as articles 31 and 32 of the Vienna Convention*
> *on the Law of Treaties. The notions of "power" and "effective control" are indicators of whether a State is exercising "jurisdiction" or governmental powers, the abuse of which human rights protections are*

> *intended to constrain. A State cannot avoid its human rights responsibilities simply by refraining from bringing those powers within the bounds of law. To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other.»*

2. Zu beachten sei auch das Diskrimierungsverbot ("The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights [A/HRC/27/37] vom Juni 2014 [http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc]):

> *«23. [...] Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.»*

3. Das Vorgehen von Geheimdiensten, auf «ausländische» Daten zu zielen bzw. Daten, welche ohnehin regelmässig (auch) im Ausland unterwegs sind, als «ausländisch» zu betrachten, führt zu einem geschwächten oder gar inexistenten Schutz der Privatsphäre für Ausländern gegenüber den eigenen Bürgern. Dies ist mit Blick auf das Diskriminierungsverbot nicht haltbar. Im Report of the Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age" (A/HRC/27/37) vom Juni 2014 (http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc) wird dazu ausgeführt (m.w.H.):

> *«35. This conclusion is equally important in the light of ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security surveillance oversight regimes. Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside, or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some*

point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.

36. International human rights law is explicit with regard to the principle of non-discrimination. Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks", as well as with article 2, paragraph 1. In this regard, the Human Rights Committee has underscored the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."»

4. Die Funk- und Kabelaufklärung verletzen das Diskriminierungsverbot nicht nur im Hinblick auf die Ungleichbehandlung von in- und ausländischen Personen. Vielmehr ist beim heutigen Stand der Technik von sprachbearbeitenden Systemen der künstlichen Intelligenz unvermeidbar, dass diese automatisch lernenden Systeme durch die Beschäftigung mit den bearbeiteten Daten diskriminierende Vorurteile erlernen (siehe z.B. Caliskan, Bryson, Narayanan: Semantics derived automatically from language corpora contain human-like biases. Science Vol 356, Issue 6334, 14 April 2017). Die Verwendung solcher Systeme zur Analyse von Kommunikationsdaten der Massenüberwachung ist darum unvermeidbarweise ein Verstoss gegen das Prinzip, dass jegliche Eingriffe in Menschenrechte frei von Diskriminierung aufgrund von Rasse, Religion, Geschlecht usw. sein müssen. Bei der Funk- und Kabelaufklärung geht es ja gerade nicht um eine gezielte Überwachung von aufgrund objektiv überprüfbarer Kriterien bestimmten, aus irgendeinem objektiven Grund verdächtigen Personen, sondern die zu vertiefter Analyse führenden Hits werden durch ein automatisiertes System generiert, das aus den

bearbeiteten Sprachdaten Vorurteile erlernt hat und das darum das Diskriminierungsverbot verletzt.

L. Internationaler Austausch

1. Das NDG sieht die Bekanntgabe von Personendaten ans Ausland vor, einschliesslich Daten, welche aus der Funk- und Kabelaufklärung gewonnen werden (Art. 61 NDG). Tatsächlich wird es wie bei anderen Datenbeschaffungen des NDB ein zentraler Aspekt der Funk- und Kabelaufklärung sein, auf dem internationalen Datenmarkt zwischen den Nachrichtendiensten verschiedener Länder genügend selbst gewonnene Daten anbieten zu können. Umgekehrt kann der NDB so auch wieder Daten von ausländischen Stellen erhalten. Schon im GPDel-Bericht vom 10. November 2003 wird festgestellt, dass die dank Onyx empfangenen Informationen auch ein nützliches «Tauschmittel» mit den entsprechenden Dienststellen im Ausland bilden. Diese Beziehungen würden auf der Grundlage eines gegenseitigen Gebens und Nehmens basieren, d.h. nach dem Prinzip des «do ut des». Die schweizerischen Dienste könnten nur dann hoffen, von ihren Partnern Informationen zu erhalten, wenn sie ihnen als Gegenleistung ebenfalls interessante Informationen anzubieten hätten. Die mit Hilfe von Onyx eingeholten Informationen seien deshalb auch ein Instrument, mit dem die Türen zu anderen Nachrichtendiensten geöffnet werden können (GPDel-Bericht vom 10. November 2003, Ziff. 5.1.1). Zwar hat der NDB vor jeder Bekanntgabe zu prüfen, ob die rechtlichen Voraussetzungen für die Bekanntgabe erfüllt sind, und die Bekanntgabe wird an gewisse Voraussetzungen geknüpft. Die diesbezüglichen Einschränkungen sind aber viel zu vage formuliert und orientieren sich zu sehr am Bedarf nach Datenaustausch und viel zu wenig an den Grundrechten der vom Datenaustausch Betroffenen. Zureichende, griffige Voraussetzungen, welche die Einhaltung der Grundrechte bei der Datenbekanntgabe ins Ausland zu gewährleisten vermögen, bestehen nicht. Nicht zu leugnen ist schliesslich die bei diesem internationalen Datenaustausch bestehende Tendenz, sich Daten dort beschaffen zu lassen, wo dies möglich ist, insbesondere aufgrund eines schwächeren Schutzes der Privatsphäre. Auch Einschränkungen, welche in Bezug auf die Überwachung von Inländern bestehen, lassen sich umgehen, indem die entsprechende Überwachung einem ausländischen Dienst überlassen wird, dem man allenfalls wiederum Daten anbieten kann, die dieser seinerseits aufgrund der für ihn bestehenden Restriktionen nicht gewinnen kann.

2. Diese Mechanismen sind auch vom Office of the United Nations High Commissioner for Human Rights als ungesetzlich kritisiert worden, weil Überwachungsmassnahmen auf diese Weise für jene, welche von ihnen betroffen sind, unvorhersehbar sind. Es hält im Report "The right to privacy in the digital age"A/HRC/27/37 vom Juni 2014 (http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc) fest:

> *«30. The requirement of accessibility is also relevant when assessing the emerging practice of States to outsource surveillance tasks to others. There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it. […]»*

M. Keine Information über Datenbearbeitung, kein Recht auf Benachrichtigung

1. Wer von der Funk- und Kabelaufklärung betroffen ist, wird in aller Regel nie davon erfahren. Die Ausleitung und Filterung von Datenströmen erfolgt heimlich. Generiert die Suche Hits und werden die entsprechenden Daten dann weiter bearbeitet, so werden die Betroffenen hierüber während der laufenden Bearbeitung nicht orientiert. Eine spätere Orientierung von Amtes wegen ist ebenfalls nicht vorgesehen. Das datenschutzrechtliche Auskunftsrecht ist stark eingeschränkt (Art. 63 ff. NDG) und vermag den diesbezüglichen Ansprüchen a priori nicht zu genügen. Vor allen Dingen wird es bezüglich der Funk- und Kabelaufklärung insoweit nicht zum Tragen kommen können, als die Massenüberwachung bereits einsetzt, bevor bzw. ohne dass beim NDB Daten vorhanden sind, die er auf Gesuch einer betroffenen Person herausgeben kann. Die Datenbearbeitung erfolgt zunächst automatisiert aufgrund von Stichworten. Der NDB kann nicht wissen, wen diese Datenbearbeitung alles betrifft und wird dem entsprechend allein über diese Datenbearbeitung der gesuchstellenden Person nicht Auskunft darüber geben können. Hits werden dann zwar vom ZEO und vom NDB bearbeitet werden. Dabei wird aber oft unklar bleiben, auf welche konkrete Person sich diese Daten beziehen, da die Daten nicht zielgerichtet von bestimmten Personen gewonnen werden, sondern aus einer Massenüberwachung stammen, und deren Inhalt und Tragweite regelmässig nicht ohne Weiteres klar sein wird.

2. Schliesslich ist generell festzustellen, dass die Heimlichkeit der Überwachung und die an verschiedenen Stellen hervorgehobene fehlende Vorhersehbarkeit dieser Massnahme ein kaum überwindbares Hindernis gegen eine effektive Datenauskunft bildet. Nachdem sich niemand ein Bild

davon machen kann, in wie weit er konkret Ziel der Funk- und Kabelaufklärung ist, wir

N. Schlussfolgerungen

1. Die Funk- und Kabelaufklärung lässt sich aufgrund ihres breiten Ansatzes, der zwangsläufig zu einer Massenüberwachung führt, nicht realisieren, ohne die Grundrechte zahlreicher Personen und insbesondere die Grundrechte der GesuchstellerInnen zu verletzen. Die GesuchstellerInnen sind in ihrem Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]), in ihrer Freiheit der Meinungsäusserung, in ihrer Meinungs- und Informations- sowie Medienfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II) und Versammlungsfreiheit (Art. 22 BV, Art. 11 EMRK), in ihrer persönlichen Freiheit und Bewegungsfreiheit (Art. 10 Abs. 2 BV, Art. 8 EMRK), im Berufsgeheimnis i.S.v. Art. 321 StGB bzw. dem Schutz der Kommunikation zwischen den GesuchstellerInnen und allfälligen BerufsgeheimnisträgerInnen, in der Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV) und Medienfreiheit und dem Anspruch auf journalistischen Quellenschutz (Art. 17 BV, Art. 10 EMRK) verletzt. Damit erscheint es zur Wahrung der Grundrechte der GesuchstellerInnen als erforderlich, vom der Durchführung der Funk- und Kabelaufklärung abzusehen.

2. Der Betrieb der Funk- und Kabelaufklärung durch den NDB und weiteren Stellen, namentlich durch das Zentrum für elektronische Operationen der Armee (ZEO) sowie jegliche Tätigkeiten, die dem Betrieb der Funkaufklärung und Kabelaufklärung dienen, ist deshalb zu unterlassen.

3. In die Funk- und Kabelaufklärung sind verschiedene Stellen involviert. Zur ausreichenden Gewährleistung hat der NDB darum jegliche in den Betrieb der Funk- und Kabelaufklärung involvierten Stellen und Personen anzuweisen, ihre diesbezügliche Tätigkeit zu unterlassen.

4. Funkaufklärung wird bereits seit vielen Jahren betrieben; die Kabelaufklärung soll ab dem Zeitpunkt der Inkraftsetzung des NDG am 1. September 2017 betrieben werden können. Die GesuchstellerInnen sind insoweit konkret in ihren Grundrechten tangiert. Der Klarheit halber und zur Wahrung der tangierten Grundrechte ist vom NDB festzustellen, dass die Funk- und Kabelaufklärung die GesuchstellerInnen in ihren Grundrechten verletzt, namentlich in ihrem Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung

(Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]), in ihrer Freiheit der Meinungsäusserung, in ihrer Meinungs- und Informationssowie Medienfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II) und Versammlungsfreiheit (Art. 22 BV, Art. 11 EMRK), in ihrer persönlichen Freiheit und Bewegungsfreiheit (Art. 10 Abs. 2 BV, Art. 8 EMRK), im Berufsgeheimnis i.S.v. Art. 321 StGB bzw. dem Schutz der Kommunikation zwischen den GesuchstellerInnen und allfälligen BerufsgeheimnisträgerInnen, in der Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV) und Medienfreiheit und dem Anspruch auf journalistischen Quellenschutz (Art. 17 BV, Art. 10 EMRK). Insbesondere die in der EMRK verankerten Grundrechte gewähren der betroffenen Person u.a. auch einen Anspruch auf Feststellung einer Grundrechtsverletzung.

Abschliessend ersuche ich Sie um Gutheissung der eingangs gestellten Anträge.

Mit freundlichen Grüssen

Viktor Györffy

Beilagen:
1. Vollmacht der Gesuchstellerin 1 in Kopie
2. Vollmacht des Gesuchstellers 2 in Kopie
3. Vollmacht des Gesuchstellers 3 in Kopie
4. Vollmacht der Gesuchstellerin 4 in Kopie
5. Vollmacht der Gesuchstellerin 5 in Kopie
6. Vollmacht des Gesuchstellers 6 in Kopie
7. Vollmacht des Gesuchstellers 7 in Kopie
8. Vollmacht des Gesuchstellers 8 in Kopie
9. Statuten der Gesuchstellerin 1 in Kopie