



CH-3003 Bern NDB

**Einschreiben**

Bundesverwaltungsgericht / Abteilung I  
Frau Instruktionsrichterin Kathrin Dietrich  
Postfach  
9023 St. Gallen

Referenz/Aktenzeichen: A-6143/2017  
Ihr Zeichen: dik/mep/dik  
Unser Zeichen: Zip / Bup  
Bern, 12. Januar 2018

A-6143/2017  
15. JAN. 2018

|         |         |          |         |         |
|---------|---------|----------|---------|---------|
| Abt. I  | Abt. II | Abt. III | Abt. IV | Abt. V  |
| Abt. VI |         | PR       | GS      | JURIDIK |
| DIK     | KOB     | HR + O   | FI/CO   | WD      |
|         |         | BESI     | ZK      |         |

**Geschäfts-Nr. A-6143/2017 / Vernehmlassung**

Sehr geehrte Frau Instruktionsrichterin

In rubrizierter Angelegenheit übermitteln wir Ihnen hiermit frist- und formgerecht unsere

**VERNEHMLASSUNG**

**Rechtsbegehren**

Die Beschwerde sei abzuweisen.

**Materielles**

Die Ausführungen des Beschwerdeführers werden bestritten, sofern sie nicht explizit anerkannt werden. Im Übrigen enthält die Beschwerde keine neuen Tatsachen oder Beweismittel, die ein Zurückkommen auf unsere Verfügung rechtfertigen würden. Es kann deshalb grundsätzlich auf die Ausführungen in der angefochtenen Verfügung verwiesen werden. Ergänzend dazu Folgendes:

Nach Artikel 25a des Verwaltungsverfahrensgesetzes (VwVG; SR 172.021) kann, wer ein schutzwürdiges Interesse hat, den Erlass einer Verfügung über Realakte verlangen. Der Nachweis eines schutzwürdigen Interesses obliegt dem Gesuchsteller. Wird weder ein Rechtsschutzbedürfnis dargelegt, noch ergibt sich ein solches aus den Akten, ist auf das Rechtsschutzansuchen nicht einzutreten.

Die Gesuchsteller legen weder einen „Sondernachteil“ dar, noch ergibt sich ein solcher aus den Akten. Bezeichnenderweise haben sie davon abgesehen, ein datenschutzrechtliches Einsichtsgesuch zu stellen und mit entsprechenden Einträgen ein schutzwürdiges Interesse zu dokumentieren. Sie sind deshalb nicht mehr als jedermann von der Funk- und Kabelauf-

klärung betroffen. Überdies ergaben Abklärungen des NDB in der einschlägigen Datenbank, dass keiner der Gesuchsteller(innen) beim NDB im Zusammenhang mit einem Funk- und Kabelaufklärungsauftrag verzeichnet ist, so dass sich zum vornherein keine ihre Rechte oder Pflichten berührenden Handlungen eruieren lassen. Ihr Gesuch erweist sich damit als gegenstandslos, weshalb der NDB zu Recht nicht darauf eingetreten ist.

Aber selbst unterstellt, es würden einschlägige Handlungen vorliegen – was ausdrücklich bestritten wird-, müssten diese dem Gesetzeswortlaut zufolge widerrechtlich erfolgen. Kann das Vorliegen einer widerrechtlichen Handlung jedoch dermassen klar erkennbar, augenfällig und offenkundig wie vorliegend ausgeschlossen werden, ist das Gesuch nicht materiell abzulehnen, sondern es ist darauf nicht einzutreten. Diesbezüglich kann einerseits auf den umfassenden Gesetzgebungsprozess verwiesen werden, in dessen Ablauf zahlreiche Sicherungen eingebaut sind, die den Erlass von mit übergeordnetem Recht im Widerspruch stehenden Rechtsvorschriften verhindern (z.B. zwingende Konsultationen des Bundesamts für Justiz, Mitberichtsverfahren, obligatorische Ausführungen zur Gesetzes- und Verfassungsmässigkeit in der Botschaft oder etwa die parlamentarische Beratung).

Andererseits ergibt sich die fehlende Widerrechtlichkeit auch daraus, dass die Funk- und Kabelaufklärung in ein ausgewogenes System von „checks and balances“ eingebettet ist:

Die Funkaufklärung gibt es seit längerer Zeit; sie wird im bisherigen Rahmen weitergeführt und nach wie vor durch ein Konstrukt von klaren, ausreichenden und gut funktionierenden Bestimmungen im Bundesgesetz über den Nachrichtendienst (NDG; SR 121) und in der Verordnung über die elektronische Kriegführung und die Funkaufklärung (VEKF, SR 510.292) geregelt. In diesem Rahmen ist auch und gerade die vom Beschwerdeführer fast vollständig ausgeblendete „Unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung (UKI)“ angemessen mit zu würdigen (vgl. insbesondere die nachfolgenden Ausführungen zur Aufsicht).

Bereits die Beauftragung des die Kabelaufklärung durchführenden Dienstes (Zentrum für elektronische Operationen, ZEO) unterliegt sowohl einer richterlichen als auch einer politischen Überprüfung und Genehmigung (Art. 40 und 41 i.V.m. Art. 29 bis 32 NDG). So muss dem Bundesverwaltungsgericht ein Antrag mit im NDG definierten Angaben unterbreitet werden. Namentlich muss der Antrag die Beschreibung des Auftrages, die Begründung der Notwendigkeit des Einsatzes, die Angabe der Kategorien von Suchbegriffen (ausgeschlossen sind beispielsweise Angaben über schweizerische Personen), die Angabe der zu verpflichtenden Fernmeldediensteanbieter (muss im Einzelfall anhand der Kenntnis der Durchleitungswege durch die Schweiz festgelegt werden; die Fernmeldediensteanbieter sind verpflichtet entsprechende technische Angaben zu machen) sowie Beginn und Ende des Auftrags enthalten. Selbstredend darf die beantragte Kabelaufklärung nur der Beschaffung von sicherheitspolitisch bedeutsamen Informationen in den durch das NDG festgelegten Aufgabenbereichen des NDB und zu bestimmten, in Artikel 25 der Verordnung über den Nachrichtendienst (NDV, SR 121.1) beispielhaft aufgezählten Zwecken dienen. Dadurch wird sich ein Kabelaufklärungsauftrag stets im Rahmen einer klar umrissenen Thematik bewegen. Zudem wird durch die sorgfältige und gezielte Auswahl der Kategorien von Suchbegriffen und der zu verpflichtenden Fernmeldediensteanbieter sichergestellt, dass von Beginn weg nur Daten zur weiteren Verarbeitung gelangen, welche mit hoher Wahrscheinlichkeit auftragsrelevante Informationen enthalten. Andernfalls wäre davon auszugehen, dass das Bundesverwaltungsgericht den Antrag ohnehin nicht genehmigen würde.

Im Rahmen der Entscheidungsfindung kann das Bundesverwaltungsgericht zusätzlich eine Anhörung von Vertretern des NDB anordnen. Erteilt das Gericht die Genehmigung, so gilt diese höchstens für sechs Monate. Eine Verlängerung um jeweils höchstens drei Monate ist möglich. Nach erfolgter Genehmigung durch das Bundesverwaltungsgericht muss zusätzlich die Freigabe durch den Vorsteher des VBS eingeholt werden. Dieser entscheidet aber erst,

nachdem er sowohl die Vorsteherin des EJPD als auch den Vorsteher des EDA dazu konsultiert hat. Fälle von besonderer Bedeutung können dem Gesamtbundesrat vorgelegt werden.

Ist ein Antrag schliesslich genehmigt und freigegeben, so erteilt der NDB den entsprechenden Kabelaufklärungsauftrag an das mit der Durchführung betraute ZEO. Dieses nimmt auch sämtliche Kontakte zu den Fernmeldediensteanbietern wahr. Einerseits verfügt das ZEO sowohl über die technischen Kompetenzen und Einrichtungen, um die Kabelaufklärung erfolgreich durchführen zu können. Andererseits dient diese Auslagerung auch dem Grundrechtsschutz, da so der NDB erst zum Schluss, nachdem das ZEO alle nicht auftragskonformen Daten ausgeschieden hat, einzig die relevanten Informationen erhält.

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

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

Im Ergebnis wird somit alles unternommen, um – auch unter Kontrolle der recht- und verhältnismässigen Umsetzung der Kabelaufklärung durch die UKI sowohl beim NDB, als auch beim ZEO - auf die Nadel, und nicht auf den Heuhaufen zu fokussieren.

Sind die Informationen erst bis zum NDB gelangt, so greift ein ausgewogenes Datenerfassungs-, haltungs- und –bewirtschaftungssystem, welches insbesondere auch der Qualitätssicherung und dem Datenschutz Rechnung trägt.

Die Daten zur Steuerung der Funk- und Kabelaufklärung sowie Daten zum Controlling und Reporting werden im Informationssystem Kommunikationsaufklärung (ISCO) bearbeitet (Art. 56 NDG, Art. 56 ff. der Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes, VIS-NDB; SR 121.2). Es werden also lediglich das Target (i.d.R. Telefonnummer), die Identitätsdaten der Zielperson sowie der Auftrag an FUB ZEO in ISCO erfasst. Dies ist notwendig, um Steuerung und – auch und gerade zum Schutz der Betroffenen - Compliance lückenlos sicherzustellen.

Die Resultate der Funk- und Kabelaufklärung werden vom Sensor (z.B. Mitarbeiter des FUB ZEO) auf den Aufgabenbezug nach Artikel 6 NDG hin geprüft, in Form eines Berichts an den NDB übermittelt und in das integrale Analysesystem IASA NDB (Art. 49 NDG, Art. 16ff. VIS-NDB), in das integrale Analysesystem Gewaltextremismus IASA-GEX NDB (Art. 50 NDG, Art. 22 ff. VIS-NDB) oder in den Restdatenspeicher (Art. 57 NDG, Art. 61 ff. VIS-NDB) abgelegt.

In ISCO werden die Aufklärungsaufträge und die Datenbestände jährlich unter Berücksichtigung der aktuellen Lage auf ihre Zweckmässigkeit und Verhältnismässigkeit hin überprüft. Diese Prüfung wird durch die für die Datenablage zuständigen Mitarbeiterinnen und Mitarbeiter des NDB durchgeführt. Nicht mehr benötigte Daten zu abgeschlossenen Aufklärungsauf-

trägen werden gelöscht, als unrichtig erkannte Daten werden berichtigt, gekennzeichnet oder gelöscht (Art. 45 Abs. 4 NDG, Art. 59 VIS-NDB). Zusätzlich führt die Qualitätssicherungsstelle des NDB mindestens einmal jährlich eine Stichprobe durch und prüft dabei die Rechtmässigkeit, Zweckmässigkeit, Wirksamkeit und Richtigkeit der Datenbearbeitung (Art. 11 Abs. 2 VIS-NDB).

Die maximale Aufbewahrungsdauer von Daten in ISCO beträgt höchstens fünf Jahre nach Abschluss des entsprechenden Aufklärungsauftrages. Die Aufbewahrung der Daten über die Dauer des Aufklärungsauftrages hinaus ist absolut notwendig, damit die Unabhängige Kontrollinstanz (UKI) – auch und gerade zum Schutz der Betroffenen - ihre Kontrolltätigkeit umfassend wahrnehmen kann.

Um den Datenschutz der betroffenen Personen bestmöglich zu wahren, ist der Kreis der zugriffsberechtigten Personen auf ISCO so klein wie möglich gehalten. Es haben nicht alle Mitarbeitenden des NDB Zugriff, sondern lediglich diejenigen Stellen, die diesen zur Aufgabenerfüllung benötigen (Art. 58 Abs. 2 und Anhang 11 VIS-NDB).

In IASA NDB werden die Daten aus den folgenden Bereichen abgelegt, erfasst und ausgewertet: Terrorismus, verbotener Nachrichtendienst, Weiterverbreitung nuklearer, biologischer oder chemischer Waffen, einschliesslich ihrer Trägersysteme, sowie aller zur Herstellung dieser Waffen notwendigen zivil und militärisch verwendbaren Güter und Technologien (NBC-Proliferation) oder dem illegalen Handel mit radioaktiven Substanzen, Kriegsmaterial und anderen Rüstungsgütern, Angriffen auf Informations-, Kommunikations-, Energie-, Transport- und weiteren Infrastrukturen, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen), Beobachtung und Beurteilung von sicherheitspolitisch bedeutsamen Vorgängen im Ausland, Wahrung der Handlungsfähigkeit der Schweiz sowie Wahrung weiterer wichtiger Landesinteressen nach Artikel 3 NDG, wenn dafür ein konkreter Auftrag des Bundesrates vorliegt (Art. 49 i.V.m. Art. 6 Abs. 1 NDG). Die Daten über den gewalttätigen Extremismus werden nicht in IASA NDB bearbeitet.

Auch in IASA NDB gelten umfangreiche Qualitäts- und Datenschutzvorschriften. Bereits bei der Erfassung beurteilen die zuständigen Mitarbeiterinnen und Mitarbeiter des NDB die Erheblichkeit und Richtigkeit der zu erfassenden Personendaten und kennzeichnen Quelldokumente, die gestützt auf Artikel 5 Absatz 6 NDG erhoben wurden (die Rechte über die politische Betätigung und über die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit in der Schweiz werden ausgeübt, um terroristische oder verbotene nachrichtendienstliche Tätigkeiten vorzubereiten) oder als Des- oder Falschinformation beurteilt werden und sie für die Beurteilung der Lage oder einer Quelle notwendig sind.

Zudem werden alle Daten periodisch durch die für die Datenerfassung zuständigen Mitarbeiterinnen und Mitarbeiter geprüft. Dabei prüfen sie unter Berücksichtigung der aktuellen Lage, ob der Personendatensatz für die Erfüllung der Aufgaben des NDB nach Artikel 6 NDG noch notwendig ist und wiederum ob die Datenbearbeitungsschranke von Artikel 5 Absätze 5 und 6 NDG eingehalten wird. Nicht mehr benötigte Daten werden gelöscht, als unrichtig erkannte Daten werden berichtigt, gekennzeichnet oder gelöscht (Art. 20 VIS-NDB). Zusätzlich führt die Qualitätssicherungsstelle NDB jährlich eine Stichprobe durch und überprüft die Rechtmässigkeit, Zweckmässigkeit, Wirksamkeit und Richtigkeit der Datenbearbeitung (Art. 45 NDG, Art. 11 VIS-NDB).

Die Zugriffsberechtigungen sind auf Mitarbeitende des NDB beschränkt. Externe Stellen (mit Ausnahme der Mitarbeitenden der unabhängigen Aufsichtsbehörde nach Art. 76 NDG) haben keinen Zugriff auf IASA NDB.

IASA-GEX NDB dient der Erfassung, Bearbeitung und Auswertung von Informationen, die den gewalttätigen Extremismus betreffen. Diese Datenbank wird hier mehr der Vollständigkeit halber aufgeführt, da gewalttextremistischen Gruppierungen kaum je von der Funk- und

Kabelaufklärung betroffen sein dürften. Die Informationen dürfen nur zu den in den Artikeln 25 NDV bzw. Art. 3 VEKF genannten Zwecken beschafft werden und dabei dürfte lediglich in einzelnen und äusserst seltenen Fällen ein Bezug zum gewalttätigen Extremismus bestehen.

Im Restdatenspeicher schliesslich werden alle Informationen abgespeichert, die bei der Triage nach der Eingangsprüfung nicht einem anderen System zugewiesen werden konnten (vgl. dazu Art. 57 NDG, Art. 61 ff. VIS-NDB). Dabei kann es sich auch um Daten aus der Funk- und Kabelaufklärung handeln.

Bei der Ablage der Daten prüfen die zuständigen Mitarbeiter ob genügend Anhaltspunkte bestehen, dass der Aufgabenbezug nach Artikel 6 NDG gegeben ist, die Datenbearbeitungsschranke nach Artikel 5 Absatz 5 NDG eingehalten wird und ob die in den Originaldokumenten enthaltenen Informationen aufgrund der Quellenqualität und der Übermittlungsart richtig und erheblich sind. Wenn darüber Zweifel bestehen, wird das betreffende Originaldokument inhaltlich geprüft. Fällt die Prüfung negativ aus, so werden die Originaldokument vernichtet oder, wenn sie von einer kantonalen Vollzugsbehörde stammen, zurückgeschickt.

Daten, welche für die Aufgabenerfüllung des NDB benötigt werden, sind in IASA NDB, IASA-GEX NDB oder GEVER zu überführen und können im Restdatenspeicher vernichtet werden. Sollen Personendaten verwendet oder weitergegeben werden, dann gelten für die Überführung die Bestimmungen von Artikel 4 Absatz 1 VIS-NDB. Es werden also wiederum der Aufgabenbezug nach Artikel 6 NDG sowie die Richtigkeit und Erheblichkeit der zu erfassenden Personendaten geprüft. Dabei ist die Datenbearbeitungsschranke nach Artikel 5 Absatz 5 NDG zu berücksichtigen. Fällt diese Prüfung negativ aus, werden die Daten vernichtet oder zurückgeschickt, wenn sie von einer kantonalen Vollzugsbehörde stammen.

Eine periodische Überprüfung durch die Mitarbeitenden von Daten im Restdatenspeicher ist wenig sinnvoll, da die Daten hier nur abgelegt, noch keinem Bereich zugeordnet und nicht personenbezogen erfasst werden. Deshalb wurde auf dieses Instrument verzichtet und stattdessen die Aufbewahrungsfrist drastisch gekürzt (5 Jahre; Art. 65 VIS-NDB). Die Qualitätssicherungsstelle des NDB führt dennoch jährlich eine Stichprobenkontrolle durch, wobei sie die Rechtmässigkeit, Zweckmässigkeit, Wirksamkeit und Richtigkeit der Datenbearbeitung. Die Zugriffsrechte sind auch beim Restdatenspeicher auf Mitarbeitende des NDB beschränkt, externe Personen oder Behörden haben keinen Zugriff (mit Ausnahme der Mitarbeitenden der unabhängigen Aufsichtsbehörde).

Für alle Informationssysteme des NDB gilt selbstverständlich ein Auskunftsrecht. Unter anderem für die Systeme ISCO, IASA NDB, IASA-GEX NDB und den Restdatenspeicher gelten spezialgesetzliche Regelungen (Art. 63 NDG), worauf verwiesen werden kann.

Sobald das Geheimhaltungsinteresse weggefallen ist oder spätestens beim Ablauf der Aufbewahrungsfrist, erteilt der NDB der gesuchstellenden Person nach dem Datenschutzgesetz Auskunft. Personen, über die keine Daten bearbeitet wurden, informiert der NDB spätestens drei Jahre nach Eingang ihres Gesuchs über ihre Nichtverzeichnung.

Das NDG hat umfangreiche Bestimmungen zur Weitergabe von Personendaten an andere Stellen (Art. 59 – 62 NDG, Art. 32 – 35 NDV). Vor jeder Weitergabe von Personendaten oder deren Verwendung in Produkten stellen die Mitarbeitenden des NDB sicher, dass die Personendaten den rechtlichen Vorgaben nach dem NDG genügen, die Weitergabe rechtlich vorgesehen und im konkreten Fall notwendig ist.

Die Weitergabe an inländische Behörden ist nur dann zulässig, wenn dies zur Wahrung der inneren oder äusseren Sicherheit notwendig ist. Den Strafverfolgungsbehörden werden die Daten zur Verhinderung von schweren Straftaten oder zur Aufrechterhaltung der öffentlichen Ordnung zur Verfügung gestellt. Anderen inländischen Behörden werden Personendaten nur unter den in Anhang 3 der NDV aufgeführten Zwecken weitergegeben.

Die Weitergabe von Personendaten an ausländische Behörden erfolgt nur unter strengen gesetzlichen Regelungen. So ist vor jeder Weitergabe genau zu prüfen, ob die rechtlichen Voraussetzungen eingehalten werden. Wenn die Gesetzgebung des Empfängerstaates keinen angemessenen Datenschutz gewährleistet, dürfen Personendaten nur bekanntgegeben werden, wenn die Schweiz mit ihm diplomatische Beziehungen pflegt und die Schweiz aufgrund eines Gesetzes oder eines völkerrechtlichen Vertrags dazu verpflichtet ist, dies zur Wahrung eines überwiegenden öffentlichen Sicherheitsinteresses der Schweiz oder des Empfängerstaates wie der Verhinderung oder Aufklärung einer auch in der Schweiz strafbaren schweren Straftat notwendig ist, dies zur Begründung eines Ersuchens der Schweiz um Information notwendig ist (z.B. die Personensicherheitsprüfung einer in der Schweiz lebenden Person) oder die Weitergabe im Interesse der betroffenen Person liegt und diese der Weitergabe zugestimmt hat oder deren Zustimmung nach den Umständen eindeutig angenommen werden kann sowie wenn die Weitergabe zum Schutz von Leib und Leben von Dritten notwendig ist.

Im Einzelfall können Personendaten an Staaten bekanntgegeben werden, mit denen die Schweiz diplomatische Beziehungen pflegt, und der ersuchende Staat schriftlich zusichert, über das Einverständnis der betroffenen Person zu verfügen und dem ersuchenden Staat dadurch eine Sicherheitsprüfung der betroffenen Person ermöglicht wird.

Wenn Staaten ein angemessenes Datenschutzniveau gewährleisten können und mit denen die Schweiz einen Vertrag nach Artikel 70 Absatz 3 abgeschlossen hat, können Personendaten ausländischen Sicherheitsorganen im Abrufverfahren bekannt gegeben werden.

Die empfangende Stelle wird durch den NDB darauf hingewiesen, für welchen Zweck die Daten ausschliesslich verwendet werden dürfen und dass sich der NDB vorbehält, Auskunft über die Verwendung der Daten zu verlangen.

Die Weitergabe von Personendaten ist ausgeschlossen, wenn die betroffenen Person dadurch der Gefahr der Doppelbestrafung oder ernsthafter Nachteile für Leib und Leben oder Freiheit im Sinne der EMRK oder anderen, von der Schweiz ratifizierten internationalen Abkommen ausgesetzt wird. Jede Bekanntgabe, deren Inhalt und die empfangende Stelle wird registriert und ist selbstverständlich für die Aufsichtsorgane jederzeit einsehbar.

Die Datenbekanntgabe an Dritte ist nur zulässig, wenn die betroffene Person der Weitergabe zugestimmt hat oder die Bekanntgabe zweifelsfrei im Interesse der betroffenen Person liegt, die Bekanntgabe notwendig ist, um eine schwere unmittelbare Gefahr abzuwehren oder wenn die Bekanntgabe notwendig ist, um ein Auskunftsgesuch zu begründen.

Vor diesem Hintergrund ist unbestritten, dass mit der Funk- und Kabelaufklärung Eingriffe in grundrechtlich geschützte Positionen einhergehen können. Die für solche Eingriffe nötigen Grundlagen sind jedoch im NDG auf Gesetzesstufe vorhanden und der Kerngehalt der betroffenen Grundrechte bleibt in jedem Fall gewahrt. Die Rechtfertigung des jeweiligen Grundrechtseingriffs entspricht vollumfänglich den in Artikel 36 Abs. 1 – 3 BV verankerten Kriterien. Ebenso wenig liegt eine Verletzung der EMRK vor. Insbesondere legt das NDG in Bezug auf Eingriffe in den Schutzbereich von Art. 8 EMRK hinreichend klar und für die Bürger in angemessener Weise erkennbar dar, unter welchen Bedingungen und Umständen die Behörden befugt sind, auf geheime Massnahmen zur Überwachung von Kommunikationsdiensten zurückzugreifen. Auch stellen Vorkehrungen sicher, dass die Dauer der Aufbewahrung auf das Unerlässliche beschränkt ist und erhobene Daten vor unangemessener oder missbräuchlicher Verwendung wirksam geschützt sind.

Die Einhaltung der einschlägigen Bestimmungen wird in erster Linie durch die parlamentarische Geschäftsprüfungsdelegation (GPDel), die Unabhängige Aufsichtsbehörde über die nachrichtendienstliche Tätigkeiten (AB-ND) sowie die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung sichergestellt. Derweil die GPDel über alles umfassende Befugnisse verfügt, sind die Aufgaben der AB-ND und der UKI – deren Mitglieder von Gesetzes

wegen über Fachkenntnisse in den Bereichen Telekommunikation, Sicherheitspolitik und insbesondere Grundrechtsschutz verfügen müssen und der bei Funkaufklärungsaufträgen die Rechtmässigkeitskontrolle obliegt (während Kabelaufklärungsaufträge zwingend ein Genehmigungsverfahren vor Bundesverwaltungsgericht durchlaufen müssen) - in der Verordnung über die Aufsicht über die nachrichtendienstlichen Tätigkeiten (VAND; SR 121.3) geregelt, so dass darauf verwiesen werden kann. Da mit dem Gesuch der Digitalen Gesellschaft bzw. deren Beschwerde zwangsläufig die Aussage verbunden ist, die Aufsichtsbehörden hätten versagt, wird ausdrücklich beantragt, Stellungnahmen der GPDel, der AB-ND sowie der UKI zur Frage der Zulässigkeit von Funk- und Kabelaufklärung einzuholen. Der guten Ordnung halber sei ergänzend darauf hingewiesen, dass auch die Eidg. Finanzkontrolle und in Teilbereichen der Eidg. Datenschutz- und Öffentlichkeitsbeauftragten den NDB kontrollieren, was widerrechtliches Handeln des NDB nachgerade ausgeschlossen scheinen lässt.

Alles in allem erweist sich der Nichteintretensentscheid damit als wohlbegründet.

Sollte das Gericht jedoch wider Erwarten zum Schluss gelangen, dass auf das Gesuch einzutreten und es materiell zu behandeln gewesen wäre, wird beantragt, von einer Rückweisung an den NDB abzusehen und direkt einen materiellen Entscheid zu fällen (was, soweit erkennbar, auch vom Beschwerdeführer im Subeventualbegehren sinngemäss beantragt wird). Dies weil der NDB anstelle eines Nichteintretensentscheides zwar auf das Gesuch eingetreten wäre, dieses jedoch aus den oben dargelegten Gründen erklärermassen und ohne jeden Zweifel abgewiesen hätte.

Im Übrigen übermitteln wir Ihnen beiliegend wunschgemäss die Vorakten.

Freundliche Grüsse



Dr. Paul Zinniker  
Direktor NDB a.i.

Im Doppel

Beilage/Aktenverzeichnis:

Beilage 1      Gesuch Digitale Gesellschaft vom 31. August 2017  
Beilage 2      Nichteintretensverfügung NDB vom 28. September 2017

