BVGer A-6444/2020 vom 19. November 2025

Bundesverwaltungsgericht, 2025-11-19, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bvger_A-6444_2020

FR: TAF A-6444/2020 du 19 novembre 2025

IT: TAF A-6444/2020 del 19 novembre 2025

Regeste

Datenschutz

Erwägungen

E. 1

Mit Urteil 1C_377/2019 vom 1. Dezember 2020 hat das Bundesgericht den Entscheid des Bundesverwaltungsgerichts A-6143/2017 aufgehoben und die Sache zur materiellen Beurteilung an das Bundesverwaltungsgericht zurückgewiesen; der Nachrichtendienst war auf die Begehren der Beschwerdeführenden nicht eingetreten und das Bundesverwaltungsgericht hatte mit besagtem Urteil den Nichteintretensentscheid der Vorinstanz bestätigt. Gemäss den Erwägungen des Bundesgerichts leitet sich ein Anspruch auf materielle Beurteilung aus Art. 13 EMRK ab. Die Bestimmung sei vor dem Hintergrund der Subsidiarität der Individualbeschwerde an den EGMR zu sehen und es sei aus diesem Grund jeder Person, die nach Art. 34 EMRK befugt ist, Beschwerde an den EGMR zu führen, zuvor die Möglichkeit zu geben, ihre Ansprüche von einem innerstaatlichen Gericht oder mindestens einer unabhängigen Behörde überprüfen zu lassen. Das Bundesgericht referenziert im Weiteren die Rechtsprechung des EGMR zur Beschwerdebefugnis im Zusammenhang mit geheimen Überwachungsmassnahmen und kommt in Bezug auf die Beschwerdeführenden zum Ergebnis, dass deren Opfereigenschaft grundsätzlich zu bejahen ist. Auf die Rechtsbegehren Ziffn. 1 und 2 der Beschwerdeführenden sei daher einzutreten und die Feststellungsbegehren Ziffn. 4 bis 6 seien als Eventualbegehren entgegenzunehmen. Die gebotene Prüfung, ob das geltende Regime der Funk- und der Kabelaufklärung angemessenen und wirksamen Schutz vor Missbrauch bietet, hat gemäss den Erwägungen des Bundesgerichts anhand der Prüfpunkte zu erfolgen, die der EGMR in seinem Kammerurteil Big Brother Watch und andere gegen Vereinigtes Königreich vom 13. September 2018 entwickelt hat (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 7-11). Die erwähnte Rechtssache Big Brother Watch und andere gegen Vereinigtes Königreich war zum Zeitpunkt der bundesgerichtlichen Entscheidung vor der Grossen Kammer des EGMR anhängig. Zwischenzeitlich, am 25. Mai 2021, hat diese ihr Urteil erlassen (Urteil des EGMR [Grosse Kammer] Big Brother Watch und andere gegen Vereinigtes Königreich vom 25. Mai 2021, 58170/13, 62322/14 und 24960/15). Ebenfalls am 25. Mai 2021 entscheid die Grosse Kammer die Streitsache Centrum för rättvisa gegen Schweden, die ebenfalls geheime Überwachungsmassnahmen zum Gegenstand hatte (Urteil des EGMR [Grosse Kammer] Centrum för rättvisa gegen Schweden vom 25. Mai 2021, 35252/08). Soweit fortan auf die beiden Urteile Big Brother Watch und andere und Centrum för rättvisa Bezug genommen wird, sind damit die jeweiligen Urteile der Grossen Kammer des EGMR gemeint. Die Grosse Kammer hat in den zwei Urteilen Big Brother Watch und andere und Centrum för rättvisa die von ihr zur Beschwerdebefugnis entwickelte

Praxis und damit auch die beiden Kammerurteile (implizit) bestätigt. Gemäss dem Grundsatzurteil der Grossen Kammer in Sachen Roman Zakharov gegen Russland ist hinsichtlich der Beschwerdebefugnis zu differenzieren, je nachdem, ob innerstaatlich wirksamer Rechtsschutz gegen geheime Überwachungsmassnahmen besteht. Ist dies nicht der Fall, ist jedermann, der in den Anwendungsbereich eines entsprechenden Gesetzes fällt, befugt, dagegen Beschwerde vor dem EGMR zu erheben, ohne auch nur behaupten zu müssen, konkret Opfer von Überwachungsmassnahmen geworden zu sein. Andernfalls, wenn innerstaatlich wirksamer Rechtsschutz besteht, muss die Beschwerde führende Person darlegen, mit einer hinreichenden Wahrscheinlichkeit dem Risiko einer Überwachung ausgesetzt zu sein. Das Bundesgericht hatte dies für die Beschwerdeführenden bejaht (Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 8; vgl. auch zit. Urteil Centrum för rättvisa, §§ 166 ff. unter Verweis auf das Urteil des EGMR [Grosse Kammer] Roman Zakharov gegen Russland vom 4. Dezember 2015, 47143/06, §§ 166 ff, insbes. §§ 169-171). Es besteht unter diesen Umständen kein Anlass, die Beschwerdebefugnis der Beschwerdeführenden, die im Urteilszeitpunkt gegeben sein muss, gestützt auf die beiden zwischenzeitlich ergangenen Urteile der Grossen Kammer des EGMR neu zu beurteilen. Auf die Beschwerde ist mithin im Sinne des Rückweisungsentscheids des Bundesgerichts 1C_377/2019 einzutreten und es sind die Rechtsbegehren der Beschwerdeführenden materiell zu beurteilen. Hierbei ist davon auszugehen, dass die Beschwerdeführenden zur Hauptsache die Einstellung der Funk- und Kabelaufklärung und damit ein Unterlassungsbegehren gestellt haben. Die Feststellungsbegehren der Beschwerdeführende sind entsprechend dem Rückweisungsentscheid des Bundesgerichts als Eventualanträge entgegenzunehmen (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 10). Das Bundesgericht hat in seinem Rückweisungsentscheid offen gelassen, ob Massnahmen der Funk- und Kabelaufklärung, wie die Beschwerdeführenden geltend machen, zusätzlich zum Anspruch auf Achtung des Privatlebens und der Medienfreiheit weitere Grundrechte berühren und beeinträchtigen. Darauf wird zurückzukommen sein.

E. 2

Dem Bundesverwaltungsgericht kommt bei seiner Entscheidung grundsätzlich eine uneingeschränkte Prüfungsbefugnis zu. Es überprüft insbesondere die Feststellung zum rechtserheblichen Sachverhalt und die Einhaltung von Bundes- sowie Völkerrecht. Zulässig ist auch die Rüge der Unangemessenheit (Art. 49 VwVG). Das Bundesverwaltungsgericht stellt sodann den Sachverhalt unter Vorbehalt der Mitwirkungspflicht der Parteien von Amtes wegen fest (Art. 12 und Art. 13 VwVG) und wendet das Recht grundsätzlich frei und von Amtes wegen an, ohne an die rechtliche Begründung der Parteibegehren gebunden zu sein (Art. 62 Abs. 4 VwVG). Es würdigt die Beweise grundsätzlich frei, ohne Bindung an förmliche Beweisregeln, sowie umfassend und pflichtgemäss (Urteil des BVGer A-3484/2018 vom 7. September 2021 E. 8 mit Hinweisen). Streitgegenstand

E. 3.1

Näher zu bestimmen ist zunächst der Streitgegenstand.

E. 3.2

Weist das Bundesgericht eine Angelegenheit zur Neubeurteilung an die untere Instanz zurück, so ist diese bei ihrer neuen Entscheidung an den Rückweisungsentscheid gebunden. Wie weit diese Bindung reicht, ergibt sich aus der Begründung der Rückweisung, die - abgesehen von zulässigen Noven - den Rahmen sowohl für neue Tatsachenfeststellungen

als auch für die neue rechtliche Begründung vorgibt. Neue Tatsachenfeststellungen können grundsätzlich nur zu Streitpunkten berücksichtigt werden, die Gegenstand der Rückweisung waren. Darüber hinaus ist es der unteren Instanz untersagt, der Beurteilung des Rechtsstreits einen anderen Sachverhalt zu Grunde zu legen oder die Sache unter rechtlichen Gesichtspunkten zu würdigen, die im Rückweisungsentscheid ausdrücklich abgelehnt oder überhaupt nicht in Erwägung gezogen worden sind. Die Bindungswirkung gilt für die Parteien gleichermassen; auf Begehren, die über den Gegenstand der Rückweisung hinausgehen, ist nicht einzutreten und Vorbringen, die das Bundesgericht bereits verworfen hat oder die nicht Gegenstand der Beurteilung durch das Bundesgericht waren, sind im zweiten Rechtsgang nicht mehr zu berücksichtigen (BGE 135 III 334 E. 2 und Urteil des BGer 2C_890/2018 vom 18. September 2019 E. 3.2 f., je mit Hinweisen; Urteil des BVGer A-5464/2023 vom 7. Januar 2025 E. 3.2 mit Hinweisen auf die Rechtsprechung).

E. 3.3.1

Die Beschwerdeführenden verlangen mit ihren Rechtsbegehren Ziffn. 1 und 2 gemäss dem Schreiben vom 31. August 2017 die Unterlassung der Funk- und Kabelaufklärung. Zudem sei die Verletzung von Grund- und Konventionsrechten festzustellen (Rechtsbegehren Ziffn. 4-6 gemäss dem Schreiben vom 31. August 2017).

E. 3.3.2

Nach den Erwägungen des Bundesgerichts im Rückweisungsentscheid sind die Unterlassungsansprüche der Beschwerdeführenden auf Art. 25 aDSG zu stützen (vgl. vorstehend Sachverhalt Bst. C.b). Gemäss Abs. 1 dieser Bestimmung könne, wer ein schutzwürdiges Interesse habe, vom verantwortlichen Bundesorgan verlangen, dass es das widerrechtliche Bearbeiten von Personendaten unterlässt (Bst. a), die Folgen eines widerrechtlichen Bearbeitens beseitigt (Bst. b) oder die Widerrechtlichkeit des Bearbeitens feststellt (Bst. c). Die Bestimmung gebe mithin einen Anspruch auf Unterlassung, Folgenbeseitigung und - subsidiär - auf Feststellung der Widerrechtlichkeit (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 5.2). Das Bundesgericht liess die Frage, ob den Beschwerdeführenden - in Abgrenzung zur Popularbeschwerde - im Sinne von Art. 25 Abs. 1 aDSG ein schutzwürdiges Interesse an den gestellten Begehren zukomme, letztlich offen (vgl. vorstehend Sachverhalt Bst. C.b). Es erwog, das Erfassen, Durchsuchen, Speichern und Weiterleiten von Daten stelle einen Eingriff in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung dar, die durch Art. 8 EMRK und Art. 13 BV geschützt seien; die erforderliche minimale Intensität werde bereits mit dem Erfassen und Durchsuchen erreicht. Im Rahmen der Funk- und der Kabelaufklärung würden zudem breite Funk- und Datenströme erfasst, womit das Risiko bestehen, dass auch Daten der Beschwerdeführenden bearbeitet würden. Sofern Kommunikationen von Medienschaffenden betroffen seien, sei ferner auch Art. 10 EMRK und Art. 17 BV berührt. Es bestehe mithin eine hinreichende Wahrscheinlichkeit (probabilité raisonable), dass Daten der Beschwerdeführenden von geheimen Massnahmen der Funk- und Kabelaufklärung betroffen würden, weshalb ihre Opfereigenschaft (Art. 34 EMRK) und damit die Beschwerdebefugnis grundsätzlich zu bejahen sei (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 8). Nach den weiteren Erwägungen des Bundesgerichts ermöglichen weder das direkte datenschutzrechtliche Auskunftsrecht gemäss Art. 8 aDSG (AS 1993 II 1947 f.) noch das sogenannte indirekte Auskunftsrecht gemäss aArt. 64 f. NDG (AS 2017 4124 f.) einen wirksamen Rechtsschutz zur Durchsetzung der Ansprüche gemäss Art. 25 aDSG. Die Auskunft gestützt auf Art. 8

aDSG sei, wenn sie nicht aufgeschoben werde, beschränkt auf die verfügbaren Informationen und umfasse somit nicht den gesamten Prozess der Funk- und Kabelaufklärung. Den Beschwerdeführenden sei es mithin gestützt auf Art. 8 in Verbindung mit Art. 25 aDSG nicht möglich, konkrete, sie betreffende Massnahmen der Funk- und Kabelaufklärung anzufechten. Eine solche Überprüfung ermögliche auch das indirekte Auskunftsrecht nicht. Dieses gewährleiste keine wirksame Beschwerdemöglichkeit im Sinne von Art. 13 EMRK, sondern stelle einen objektiven Kontrollmechanismus dar, welcher den Aufschub beziehungsweise die Einschränkung des Beschwerderechts teilweise kompensieren könne (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 9.1 f.). Das Bundesgericht kommt zum Ergebnis, dass die Beschwerdeführenden unter den vorliegenden Umständen darauf angewiesen sind, das System der Funk- und Kabelaufklärung als solches überprüfen lassen zu können. Dabei handle es sich nicht um eine abstrakte Normenkontrolle. Gegenstand der Prüfung sie nicht das Gesetz als solches, sondern die (vermutete) Bearbeitung von Daten der Beschwerdeführenden im Rahmen der Funk- und Kabelaufklärung. Dies entspreche dem Vorgehen bei der Überprüfung der Speicherung und Aufbewahrung der Telekommunikationsranddaten in BGE 144 I 126. Auch in jenem Verfahren hatten die Privatpersonen verlangt, es sei die Bearbeitung ihrer Personendaten zu unterlassen. Der Dienst Überwachung Post und Fernmeldeverkehr ÜPF sei auf die Unterlassungsbegehren eingetreten und habe so eine unabhängige gerichtliche Überprüfung des Systems der sogenannten Randdatenspeicherung ermöglicht (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 9.3 f.).

E. 3.3.3

Gemäss dem Rückweisungsentscheid des Bundesgerichts sieht das geltende Recht keine Möglichkeit vor, konkrete Überwachungsmassnahmen anzufechten - und in diesem Rahmen die Funk- und Kabelaufklärung als solche vorfrageweise einer Überprüfung zuzuführen. Zwar sind, so das Bundesgericht im Weiteren, gewisse Einschränkungen des Rechtsschutzes bei geheimen Überwachungsmassnahmen zulässig. Solche Einschränkungen setzten jedoch voraus, dass das Gesamtsystem der Funk- und Kabelaufklärung den Anforderungen insbesondere von Art. 8 EMRK und Art. 13 BV genüge (vgl. auch Urteile des EGMR Leander gegen Schweden vom 26. März 1987, 9248/81, § 78-84 und Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, § 68). Die Beschwerdeführenden seien darauf angewiesen, das System der Funk- und Kabelaufklärung in der Schweiz überprüfen zu lassen. Sie müssten mithin und in Nachachtung der Subsidiarität der Individualbeschwerde an den EGMR die Möglichkeit haben, ihre Ansprüche zuvor vor einem innerstaatlichen Gericht oder mindestens einer unabhängigen innerstaatlichen Behörde geltend zu machen (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 7.2 unter Verweis auf BGE 138 I 6 E. 1.3.2). Andernfalls würde effektiver Rechtsschutz vereitelt und (damit) Art. 13 EMRK verletzt (vgl. in diesem Zusammenhang auch das zit. Urteil Klass, §§ 61 ff., insbes. § 64). Streitgegenstand des vorliegenden Verfahrens ist somit die Frage, ob die (vermutete) Bearbeitung von Daten der Beschwerdeführenden im aktuellen System der Funk- und Kabelaufklärung deren Grundrechte verletzt. Hierbei ist zu prüfen, ob das Gesamtsystem der Funk- und Kabelaufklärung den grund- und konventionsrechtlichen Anforderungen genügt. Ergibt die Prüfung, dass dieses nicht konform ist mit den konventions- und grundrechtlichen Ansprüchen der Beschwerdeführenden, so hätten diese - wie anbegehrt - Anspruch auf Unterlassung, Folgenbeseitigung und - subsidiär - auf Feststellung der Widerrechtlichkeit der (vermuteten) Bearbeitung ihrer Personendaten (vgl. zum

anwendbaren Recht nachfolgend E. 4). Anwendbares Recht

E. 4.1
In einem nächsten Schritt ist zu bestimmen, welche Rechtsgrundlagen einschlägig ist.

E. 4.2.1
Gemäss dem Rückweisungsentscheid ist zu prüfen, ob die (vermutete) Bearbeitung von Daten der Beschwerdeführenden im aktuellen System der Funk- und Kabelaufklärung deren Grundrechte verletzt. Die Rechtsbegehren der Beschwerdeführenden - allen voran das Begehren auf Unterlassung der Funk- und Kabelaufklärung - sind dabei materiellrechtliche auf Art. 25 aDSG zu stützen (Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 5 und 9.3).

E. 4.2.2
Zwischenzeitlich, am 1. September 2023, ist das totalrevidierte Datenschutzgesetz vom 25. September 2020 (DSG, SR 235.1) in Kraft getreten. Die vormals in Art. 25 aDSG festgelegten Ansprüche und das Verfahren im Zusammenhang mit einer widerrechtlichen Datenbearbeitung sind neu in Art. 41 DSG geregelt. Das totalrevidierte Datenschutzgesetz enthält in Art. 70 eine Übergangsbestimmung für laufende Verfahren. Gemäss dieser ist das totalrevidierte Gesetz nicht anwendbar auf hängige Beschwerden gegen erstinstanzliche Entscheide, die vor seinem Inkrafttreten ergangen sind. Entsprechende Fälle unterstehen dem bisherigen Recht.

E. 4.2.3
Das vorliegende Beschwerdeverfahren war zum Zeitpunkt des Inkrafttretens des totalrevidierten Datenschutzgesetzes bereits hängig; die Beschwerde datiert vom 30. Oktober 2017. Gemäss der Übergangsregelung in Art. 70 DSG ist somit die Prüfung, ob die (vermutete) Bearbeitung von Daten der Beschwerdeführenden im aktuellen System der Funk- und Kabelaufklärung deren Grundrechte verletzt, auf die vormals geltenden Bestimmungen des aDSG zu stützen. An diesem Ergebnis ändert vorerst nichts, dass mit der Totalrevision des Datenschutzgesetzes auch die datenschutzrechtlichen Bestimmungen im NDG geändert wurden und dem NDG unmittelbar keine Übergangsbestimmungen entnommen werden kann. Das NDG enthält keine abschliessende beziehungsweise umfassende datenschutzrechtliche Regelung. Vielmehr gilt dort, wo keine abweichenden Spezialbestimmungen bestehen, das DSG auch für die Vorinstanz (vgl. Botschaft vom 19. Februar 2014 zum Nachrichtendienstgesetz [nachfolgend: Botschaft NDG], Bundesblatt [BBl] 2014 2105, 2235). Unter diesen Umständen ist die Anwendung der geänderten nachrichtendienstlichen Bestimmungen ebenfalls gemäss der Übergangsbestimmung von Art. 70 DSG und nicht nach den allgemeinen intertemporalrechtlichen Grundsätzen (vgl. hierzu BGE 144 II 273 E. 2.2.4 [betreffend neue Verfahrensbestimmungen] und BGE 148 I 233 E. 4.4.1 [betreffend das materielle Recht]) zu beurteilen. Dieses Ergebnis gebietet bereits der allgemeine Grundsatz der Einheit der Rechtsordnung. Gemäss dem Rückweisungsentscheid ist die Prüfung auf das aktuelle System der Funk- und Kabelaufklärung zu beziehen (Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 9.3). Welche Bedeutung dem Wort «aktuell» beizugeben ist, ergibt sich nicht unmittelbar aus dem Rückweisungsentscheid. Es fällt jedoch in Betracht, dass das totalrevidierte Datenschutzgesetz zum Urteilszeitpunkt bereits erlassen war; Erlassdatum ist der 25. September 2020. Zudem ist der besondere Charakter der vorliegenden Prüfung zu beachten: Auf der Grundlage von Art. 13 EMRK und unter Beachtung der Subsidiarität der

Individualbeschwerde an den EGMR ist zu prüfen, ob das System der Funk- und Kabelaufklärung insgesamt den Anforderungen insbesondere von Art. 8 EMRK und Art. 13 BV genügt (Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 7.2 und 9.4). Es erscheint daher weder als vom Bundesgericht beabsichtigt noch als zweckmässig, die Prüfung - entsprechend der Übergangsbestimmung - auf das alte Recht abzustützen; die Beschwerdeführenden wären unter diesen Umständen auf ein neues Begehren um Unterlassung der Funk- und Kabelaufklärung gemäss dem geltenden Recht zu verweisen. Der Prüfung, ob die (vermutete) Bearbeitung von Daten der Beschwerdeführenden im aktuellen System der Funk- und Kabelaufklärung deren Grundrechte verletzt, ist somit gestützt auch auf das zum Urteilszeitpunkt geltende Recht vorzunehmen. Dies wurde bei der Instruktion des vorliegenden Beschwerdeverfahrens berücksichtigt. Dort, wo das vormals und gemäss der Übergangsbestimmung von Art. 70 DSG anwendbare Recht abweichende beziehungsweise insbesondere weitergehende Ansprüche gewährte, ist die Prüfung auch auf das vormalige aDSG zu stützen.

E. 4.3.1

Das NDG soll revidiert werden. Beabsichtigt ist in einem ersten Revisionspaket insbesondere eine komplette Neuregelung der Bestimmungen des vierten Kapitels zur Datenbearbeitung. Diese Änderungen gehen zurück auf Empfehlungen und Vorschläge der Geschäftsprüfungsdelegation GPDel betreffend den Umgang mit nachrichtendienstlichen Daten. Zudem sollen die Aufgaben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI an die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND übertragen werden. Die Vernehmlassung zur geplanten Gesetzesrevision fand im Jahr 2022 statt und bis Ende 2025 soll der Bundesrat die Botschaft zum ersten Revisionspaket zuhanden des Parlaments verabschieden (vgl. den Bericht des Departementes für Verteidigung, Bevölkerungsschutz und Sport VBS vom 1. Oktober 2024, < www.vbs.admin.ch > Sicherheit > Nachrichtendienst > Nachrichtendienstgesetz, abgerufen am 16. Oktober 2025).

E. 4.3.2

Die parlamentarischen Beratungen zur Revision des NDG haben noch nicht begonnen. Der im Rahmen der Vernehmlassung vorgelegte Gesetzesentwurf vermag daher von vornherein keine - grundsätzlich ohnehin unzulässige - Vorwirkung zu entfalten (vgl. zur Vorwirkung BGE 149 IV 135 E. 2.4 und Urteil des BGer 1B_221/2023 vom 23. Mai 2023 E. 1.2.4 mit Hinweisen). Vorarbeiten zu Gesetzesentwürfen, die noch nicht in Kraft getreten sind, können bei der Auslegung einer geltenden Gesetzesbestimmung unter Umständen berücksichtigt werden. Dabei handelt es sich um eine Ausprägung der geltungszeitlichen Auslegung. Eine solche Berücksichtigung ist jedoch nur möglich, wenn das geltende System nicht grundsätzlich geändert, sondern nur eine Konkretisierung des bestehenden Rechtsverhältnisses angestrebt wird oder Lücken des geltenden Rechts ausgefüllt werden sollen; die Vorarbeiten können unter solchen Umständen (unter geltungszeitlichen Gesichtspunkten) zum Verständnis des geltenden Rechts beitragen (vgl. Urteile des BGer 4A_84/2021 vom 2. Februar 2022 E. 5.2.1 und 2C_784/2018 vom 11. November 2019 E. 5.7, je mit Hinweisen u.a. auf BGE 141 II 297 E. 5.5.3; zur sogenannten authentischen Interpretation, das heisst der Berücksichtigung künftigen Rechts im Rahmen der Rechtsprechung vgl. Urteil des BGer 1B_221/2023 vom 23. Mai 2023 E. 1.2.3).

E. 4.3.3

Gemäss dem erläuternden Bericht vom Mai 2022 zur geplanten Revision des NDG erfolgt an verschiedenen Stellen eine Konkretisierung des bestehenden Rechtszustandes (Erläuternder Bericht vom Mai 2022 zur Revision des Bundesgesetzes vom 25. September 2015 über den Nachrichtendienst [nachfolgend: Erläuternder Bericht Revision NDG], www.fedlex.admin.ch Vernehmlassungen Abgeschlossene Vernehmlassungen 2022 VBS, abgerufen am 16. Oktober 2025). Die Bestimmungen des vierten Kapitels über die Datenbearbeitung durch den Nachrichtendienst des Bundes NDB soll jedoch grundlegend neu geregelt werden. Bereits aus diesem Grund drängt sich mit Blick auf die dargestellte Rechtsprechung Zurückhaltung bei der Berücksichtigung der Vorarbeiten zum Gesetzesentwurf auf. Eine solche ist umso mehr zu üben, wenn - wie hier - erst das Vernehmlassungsverfahren durchgeführt worden ist und die parlamentarischen Beratungen noch nicht begonnen haben. Erneut ist jedoch auf den bereits erwähnten besonderen Charakter der vorzunehmenden Prüfung hinzuweisen (vgl. vorstehend E. 3.3.3 und 4.2.3). Auch wenn sich das Bundesverwaltungsgericht Zurückhaltung bei der Berücksichtigung der Vorarbeiten zum Gesetzesentwurf auferlegt, scheint es angebracht, dort, wo die geplante Revision des NDG - soweit dies gestützt auf die Vernehmlassungsunterlagen beurteilt werden kann - im Widerspruch zu den Anforderungen insbesondere gemäss Art. 8 EMRK und Art. 13 BV steht, einen entsprechenden Hinweis anzubringen. Gesetzliche Regelung der Funk- und Kabelaufklärung

E. 5.1

Die Beschwerde richtet sich gegen die Funk- und Kabelaufklärung des Nachrichtendienstes des Bundes NDB.

E. 5.2

Die Hauptaufgabe der Vorinstanz besteht im Beschaffen und Beurteilen von Informationen und deren Weitergabe an berechtigte Empfänger (vgl. Botschaft NDG, BBl 2014 2105, 2141). Die Funk- und die Kabelaufklärung sind Teil der nachrichtendienstlichen Informationsbeschaffung. Das NDG unterscheidet zunächst zwischen genehmigungsfreien (Art. 13 ff. NDG) und genehmigungspflichtigen Beschaffungsmassnahmen (Art. 26 ff. NDG) im Inland. Diese Bestimmungen gelten auch, wenn Informationen über Vorgänge im Ausland im Inland beschafft werden (Art. 36 Abs. 2 NDG). Für Beschaffungsmassnahmen im Ausland - zu denen auch die Funk- und die Kabelaufklärung gehören - gelten anderen Regeln. Sie unterliegen mit Ausnahme der Kabelaufklärung keiner Genehmigungspflicht und werden vom Nachrichtendienst des Bundes NDB in eigener Verantwortung eingesetzt. Die Funk- und Kabelaufklärung sind mithin Teil eines Spektrums von Möglichkeiten der Informationsbeschaffung und die unterschiedlichen Massnahmen können, was für die nachfolgende Beurteilung der Funk- und Kabelaufklärung zu beachten ist, zusammenwirken.

E. 5.3

Die Funkaufklärung erfasst gemäss Art. 38 Abs. 1 NDG elektromagnetische Ausstrahlungen von Telekommunikationssystemen (insbesondere Telekommunikationssatelliten und Kurzwellensender) im Ausland (vgl. Botschaft NDG, BBl 2014 2105, 2177). Sie dient der Beschaffung sicherheitspolitisch bedeutsamer Informationen über Vorgänge im Ausland und die Wahrung wichtiger Landesinteressen nach Art. 3 NDG (Art. 38 Abs. 2 NDG). Zuständig ist der Beigeladene (Art. 1 der Verordnung über die elektronische Kriegführung und die Funkaufklärung [VEKF, SR

510.292]). Der Nachrichtendienst des Bundes NDB und der Nachrichtendienst der Armee können dem Beigeladenen Funkaufklärungsaufträge für die in Art. 3 Abs. 3 VEKF genannten Zwecke erteilen (Art. 3 Abs. 1 VEKF). Eine Genehmigungspflicht und eine gesetzliche Befristung der Beschaffungsmassnahme ist nicht vorgesehen. Der Beigeladene leitet Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland an den Nachrichtendienst des Bundes NDB weiter (Art. 38 Abs. 4 Bst. a NDG). Im Rahmen der Funkaufklärung erhaltene Daten können auch Informationen über Personen im Inland enthalten. Solche Informationen darf der Beigeladene, sofern sie nicht auf eine Gefährdung der inneren Sicherheit hinweisen, nur anonymisiert an den Nachrichtendienst des Bundes NDB weiterleiten (Art. 38 Abs. 4 Bst. b und Abs. 5 NDG). Andernfalls sind die Daten über Personen und Vorgänge im Inland umgehend zu vernichten, wenn sie als solche erkannt worden sind (Art. 5 VEKF).

E. 5.4

Die Kabelaufklärung betrifft grenzüberschreitende Signale aus leitungsgebundenen Netzen (Art. 39 Abs. 1 NDG) und damit in erster Linie die Datenübertragung im Internet. Wie die Funkaufklärung dient auch die Kabelaufklärung der Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland (Art. 6 Abs. 1 Bst. b NDG). Hierzu werden bestimmte Datenströme auf internationalen Fernmeldekabeln erfasst, anhand von Suchbegriffen (Selektoren) nach Inhalten abgesucht und der Auswertung zugeführt (Botschaft NDG, BBl 2014 2105, 2178). Die Kabelaufklärung wird ebenfalls vom Beigeladenen durchgeführt (Art. 26 Abs. 1 der Nachrichtendienstverordnung [NDV, SR 121.1]). Aufträge zur Kabelaufklärung sind sodann genehmigungspflichtig (Art. 40 Abs. 1 NDG). Bevor der Nachrichtendienst des Bundes NDB dem Dienst einen Auftrag zur Kabelaufklärung erteilt, muss er die Genehmigung des Bundesverwaltungsgerichts sowie die Freigabe durch die Vorsteherin oder den Vorsteher des VBS einholen (Art. 40 Abs. 2 NDG). Die Genehmigung gilt für höchstens sechs Monate und kann um jeweils höchstens drei Monate verlängert werden (Art. 41 Abs. 3 NDG). Die Einführung der Genehmigungspflicht wird damit begründet, dass die Kabelaufklärung nur mit der Beteiligung schweizerischer Anbieterinnen von Fernmeldediensten durchgeführt werden kann, denen eine rechtsgültige Anordnung für das Weiterleiten der entsprechenden Datenströme an den Beigeladenen übergeben werden muss. Das Gesetz sieht daher ein analoges Genehmigungsverfahren wie bei den genehmigungspflichtigen Beschaffungsmassnahmen im Inland vor (Botschaft NDG, BBl 2014 2105, 2178; vgl. auch nachfolgend E. 6.3.4). Der durchführende Dienst verpflichtet die betroffenen Netzbetreiberinnen und Anbieterinnen von Fernmeldediensten, ihm die Signale zuzuleiten und von ihnen angebrachte Verschlüsselungen zu entfernen (Art. 43 Abs. 2 NDG; Art. 26 ff. NDV). Der Dienst bereitet die Signale anschliessend auf. In einem nächsten Schritt werden die verschiedenen Suchbegriffe (Personalien, Telefonnummern, IP-Adressen, Schlüsselwörter etc.), sogenannter Selektoren, auf die Daten angewendet. Hierzu kann der Dienst der Vorinstanz im Rahmen der genehmigten Kategorien von Suchbegriffen zusätzliche Suchbegriffe vorschlagen (Art. 27 Abs. 4 NDV). Angaben über schweizerische natürliche und juristische Personen sind als Suchbegriffe nicht zulässig (Art. 39 Abs. 3 NDG). Befinden sich sowohl der Sender als auch der Empfänger in der Schweiz, so ist die Verwendung der 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). Der Beigeladene leitet ausschliesslich Daten an die Vorinstanz weiter, die

Informationen zu den für die Erfüllung des Auftrags definierten Suchbegriffen enthalten (Art. 42 Abs. 2 Satz 1 NDG). Informationen über Personen im Inland dürfen grundsätzlich nur in anonymisierter Form und nur dann weitergeleitet werden, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind (Satz 2). Eine Ausnahme gilt, wenn die Daten Informationen über Vorgänge im In- oder Ausland enthalten, die auf eine konkrete Bedrohung der inneren Sicherheit der Schweiz hinweisen. In einem solchen Fall leitet der Beigeladene die Daten unverändert an die Vorinstanz weiter (Art. 42 Abs. 3 NDG).

E. 5.5

Die Bearbeitung von Personendaten durch die Vorinstanz ist im 4. Kapitel des NDG geregelt. Gemäss Art. 45 Abs. 1 NDG ist die Vorinstanz - entsprechend den allgemeinen datenschutzrechtlichen Grundsätzen - verpflichtet, die Erheblichkeit und die Richtigkeit der ihr übermittelten Personendaten zu kontrollieren, bevor sie diese in einer ihrer Informationssysteme erfasst (Art. 45 Abs. 1 Satz 1 NDG); Erkenntnisse aus der Funk- und Kabelaufklärung werden im integralen Analysesystem des NDB (IASA NDB) oder im Restdatenspeicher bearbeitet (Botschaft NDG, BBl 2014 2105, 2178). Bei der Beurteilung der Erheblichkeit und der Richtigkeit der Daten sind die Datenbearbeitungsschranken gemäss Art. 5 Abs. 5-8 NDG zu beachten (Art. 45 Abs. 2 NDG; Art. 3 Abs. 1 der Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes [VIS-NDB; SR 121.2]). Gemäss den in Art. 5 NDG festgelegten Grundsätzen der Informationsbeschaffung beschafft und bearbeitet die Vorinstanz keine Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit in der Schweiz (Abs. 5). Eine Ausnahme gilt, wenn konkrete Anhaltspunkte vorliegen, dass eine Person oder Organisation ihre Rechte ausübt, um terroristische, verbotene nachrichtendienstliche oder gewalttätig-extremistische Tätigkeiten vorzubereiten oder durchzuführen (Abs. 6) sowie zur Beurteilung der Bedrohung, die von Organisationen und Gruppierungen auf der Beobachtungsliste nach Art. 72 NDG ausgehen (Abs. 8). Das datenschutzrechtliche Auskunftsrecht (Art. 25 Abs. 1 DSG) ist teilweise spezialgesetzlich im NDG geregelt. Verlangt eine Person Auskunft darüber, ob die Vorinstanz Daten über sie bearbeitet, ist danach zu unterschieden, in welchem der nachrichtendienstlichen Informationssysteme Daten bearbeitet werden. Für das integrale Analysesystem des NDB (IASA NDB) und den Restdatenspeicher sieht Art. 63 Abs. 2 NDG die Möglichkeit eines Aufschubs der Auskunft vor. Demnach wird die Auskunft aufgeschoben, wenn und soweit überwiegende, in den Akten zu begründende Interessen an einer Geheimhaltung bestehen im Zusammenhang mit der Erfüllung einer Aufgabe nach Art. 6 NDG, einer Strafverfolgung oder einem anderen Untersuchungsverfahren (Art. 63 Abs. 2 Bst. a NDG). Ebenfalls aufzuschieben ist die Auskunft, wenn und soweit es wegen überwiegender Interessen Dritter erforderlich ist (Art. 63 Abs. 2 Bst. b NDG) oder wenn über die gesuchstellende Person keine Daten bearbeitet werden (Art. 63 Abs. 2 Bst. c NDG). Schiebt die Vorinstanz die Auskunft auf, so teilt sie dies der gesuchstellenden Person mit. Gleichzeitig weist sie die gesuchstellende Person darauf hin, dass sie das Recht hat, vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB zu verlangen, dass er prüfe, ob allfällige Daten rechtmässig bearbeitet werden und ob überwiegende Geheimhaltungsinteressen den Aufschub rechtfertigen (Art. 63 Abs. 3 NDG). Ein anderes, eigentliches Rechtsmittel besteht nicht. Der Beauftragte führt auf Verlangen die Prüfung durch und teilt der gesuchstellenden Person mit, dass entweder in Bezug auf sie keine Daten unrechtmässig bearbeitet werden, oder dass er bei der Datenbearbeitung oder

betreffend den Aufschub der Auskunft Fehler festgestellt und eine Untersuchung nach Art. 49 DSG eröffnet hat (Art. 64 Abs. 1 und 2 NDG). Die Mitteilungen der Vorinstanz und des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sind stets gleichlautend und werden nicht begründet (Art. 66 Abs. 1 NDG). Ein Rechtsmittel besteht nicht (Art. 66 Abs. 2 NDG). Besteht kein Geheimhaltungsinteresse mehr, erteilt die Vorinstanz der gesuchstellenden Person nach dem DSG Auskunft, sofern dies nicht mit übermässigem Aufwand verbunden ist (Art. 63 Abs. 4 DSG). Auch nach dem alten, bis zum Inkrafttreten des DSG geltenden Recht, führte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB auf Verlangen der gesuchstellenden Person die Prüfung durch. Er teilte dieser sodann jedoch mit, dass entweder in Bezug auf sie keine Daten unrechtmässig bearbeitet werden oder dass er bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft Fehler festgestellt und eine entsprechende Empfehlung im Sinne von Art. 27 aDSG zu deren Behebung an die Vorinstanz gerichtet hat (aArt. 64 Abs. 2 und 4 NDG [AS 2017 4124]). Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB wies die gesuchstellende Person zudem darauf hin, dass sie vom Bundesverwaltungsgericht verlangen könne, die Mitteilung oder den Vollzug der Empfehlung zu überprüfen (aArt. 64 Abs. 3 NDG). Das Bundesverwaltungsgericht führte sodann auf Verlangen die Prüfung nach aArt. 64 Abs. 3 NDG durch und teilte der gesuchstellenden Person anschliessend mit, dass sie durchgeführt worden ist (aArt. 65 Abs. 1 NDG). Kam es bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft zu Fehlern, so richtete das Bundesverwaltungsgericht eine Verfügung zu deren Behebung an die Vorinstanz. Gleiches galt, wenn die Empfehlung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB nicht befolgt wurde. Der Vorinstanz stand sodann eine Beschwerderecht gegen Verfügungen des Bundesverwaltungsgerichts zu (aArt. 65 Abs. 2 NDG). Die Mitteilungen des Bundesverwaltungsgerichts waren dabei wie jene des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB stets gleichlautend und wurden nicht begründet. Sie konnten zudem auch nach altem Recht nicht mit einem Rechtsmittel angefochten werden (aArt. 66 NDG).

E. 5.6

Nicht benötigte Daten aus Beschaffungsmassnahmen der Funk- und Kabelaufklärung vernichtet der Beigeladene so rasch wie möglich (Art. 38 Abs. 6 und Art. 42 Abs. 4 NDG). Die gewonnenen Resultate sind spätestens im Zeitpunkt der Beendigung des jeweiligen Auftrags zu löschen (Art. 4 Abs. 1 VEKF; Art. 28 Abs. 1 NDV). Die erfassten Kommunikationen sind sodann spätestens 18 Monate, Verbindungsdaten beziehungsweise Randdaten spätestens 5 Jahre nach deren Erfassung zu vernichten (Art. 4 Abs. 2 und 3 VEKF; Art. 28 Abs. 2 und 3 NDV). Die Vorinstanz ihrerseits überprüft periodisch in allen Informationssystemen, ob die erfassten Personendaten zur Erfüllung ihrer Aufgaben weiterhin notwendig sind. Nicht mehr benötigte Daten werden gelöscht und unrichtige Daten grundsätzlich korrigiert oder ebenfalls gelöscht (Art. 45 Abs. 4 NDG). Die Aufbewahrungsdauer und das Löschen von Daten ist im Verordnungsrecht geregelt (Art. 47 Abs. 2 Bst. e und f NDG). Demnach beträgt die Aufbewahrungsdauer für Daten, die im integralen Analysesystem des NDB (IASA NDB) erfasst werden, höchstens 45 Jahre (Quellendokumente) beziehungsweise 15 Jahre (Originaldokumente, die nicht mit einem Quellendokument referenziert sind; Art. 21 VIS-NDB). Ist die Aufbewahrungsdauer abgelaufen, löscht die Vorinstanz die Daten in den Informations- und Speichersystemen innerhalb von drei Monaten und bietet sie dem Schweizerischen Bundesarchiv BAR an (Art. 8 Abs. 2 VIS-NDB).

E. 5.7

Im Bereich der Funk- und Kabelaufklärung besteht - anders als bei genehmigungspflichtigen Beschaffungsmassnahmen im Inland gemäss Art. 33 NDG - keine Mitteilungspflicht nach Abschluss einer Funk- oder Kabelaufklärung; die Funk- und Kabelaufklärung sind nicht auf die Fernmeldeanschlüsse von bestimmten Personen ausgerichtet, sondern auf die Aufklärung von sicherheitspolitisch bedeutsamen Informationen in Funkausstrahlungen oder Kabelübermittlungen aus dem Ausland (Botschaft NDG, BBl 2014 2105, 2171).

E. 5.8

Die Funk- und Kabelaufklärung unterliegen gemäss Art. 79 NDG der Aufsicht durch eine verwaltungsinterne unabhängige Instanz, die unabhängige Instanz für die Funk- und Kabelaufklärung UKI. Diese prüft die Funkaufklärung auf Rechtmässigkeit und beaufsichtigt den Vollzug der genehmigten und freigegebenen Aufträge zur Kabelaufklärung (Abs. 1). Sie prüft die Aufträge an den durchführenden Dienst sowie die Bearbeitung und Weiterleitung der Informationen, die dieser erfasst hat. Dazu erhält sie von den zuständigen Stellen Zugang zu allen zweckdienlichen Informationen und Anlagen (Abs. 2). Aufgrund der Überprüfung kann sie Empfehlungen abgeben und insbesondere beim VBS beantragen, dass Aufträge zur Funkaufklärung eingestellt und Informationen gelöscht werden (Abs. 3; vgl. auch Art. 10 der Verordnung über die Aufsicht über die nachrichtendienstlichen Tätigkeiten [VAND, SR 121.3]). Überdies unterliegt die Vorinstanz der Aufsicht durch die unabhängige Aufsichtsbehörde über die nachrichtendienstliche Tätigkeit AB-ND (Art. 76-78 NDG) und der parlamentarischen Oberaufsicht durch die Geschäftsprüfungs- und die Finanzdelegation (Art. 81 Abs. 1 NDG).
Grundrechtsbeeinträchtigung

E. 6.1

Die Beschwerdeführenden machen eine Verletzung mehrerer durch die Bundesverfassung und die EMRK geschützter Grundrechte geltend. Sie rügen, das vermutete Erfassen, Durchsuchen, Speichern und Weiterleiten ihrer Daten verletze ihr Recht auf Achtung des Intim-, Privat- und Familienlebens, einschliesslich der Achtung des Brief-, Post- und Fernmeldeverkehrs, sowie ihren Anspruch auf Schutz vor Missbrauch persönlicher Daten (Art. 8 EMRK; Art. 13 BV), ihre Meinungs- und Informations- sowie die Medienfreiheit (Art. 10 EMRK; Art. 16 und 17 BV), ihre Versammlungsfreiheit (Art. 11 EMRK; Art. 22 BV), ihre persönliche Freiheit und Bewegungsfreiheit (Art. 8 EMRK; Art. 10 Abs. 2 BV) sowie die Unschuldsvermutung (Art. 6 EMRK; Art. 32 BV). Das Bundesgericht hat die Frage, welche Grundrechte berührt sind, im Rahmen der Eintretensfrage nicht abschliessend beurteilt (Rückweisungsentscheid 1C_399/2019 vom 1. Dezember 2020 E. 8.1). Im Folgenden ist daher zunächst auf die Schutzbereiche der als verletzt gerügten Grund- und Konventionsrechte einzugehen (nachfolgend E. 6.2). Anschliessend ist zu prüfen, ob die in Frage stehende Funk- und Kabelaufklärung die (sachlichen) Schutzbereiche der als verletzt gerügten Grund- und Konventionsrechte berührt und zudem die für eine Beeinträchtigung der grundrechtlichen Ansprüche notwendige minimale Intensität (vgl. Art. 35 Ziff. 3 Bst. b EMRK) erreicht wird (nachfolgend E. 6.3). Gegebenenfalls wird sodann zu prüfen sein, ob die Beeinträchtigung gerechtfertigt werden kann oder ein unzulässiger Eingriff vorliegt (nachfolgend E. 7 ff.; vgl. zur Terminologie des EGMR [«ingérence» bzw. «interference»] die Überschriften zu den §§ 324 ff. im zit. Urteil Big Brother Watch und andere; zudem zur Unterscheidung zwischen [sachlichem]

Schutzbereich und Grundrechtsbeeinträchtigung Christoph Raess, Die Grundrechtsbeeinträchtigung, 2020, Rz. 182 ff, insbes. Rz. 208 ff. und Rz. 223 ff., je mit Hinweisen).

E. 6.2.1

Im Vordergrund der Beschwerde steht die Rüge der Verletzung des Anspruchs auf Achtung des Privatlebens beziehungsweise - in der Terminologie der Bundesverfassung - der Privatsphäre. Die EMRK verankert in Art. 8 Ziff. 1 namentlich den Anspruch jeder Person auf Achtung ihres Privat- und Familienlebens sowie ihrer Korrespondenz. Im Wesentlichen derselbe Schutz ergibt sich aus Art. 17 des Internationalen Paktes über bürgerliche und politische Rechte (SR 0.103.2; nachfolgend: UNO-Pakt II) und Art. 13 Abs. 1 BV. Der Begriff des Privatlebens ist weit zu fassen und keiner abschliessenden Definition zugänglich. Das Recht auf Achtung des Privatlebens umfasst in sachlicher Hinsicht insbesondere die Möglichkeit, Beziehungen zu anderen Menschen aufzubauen und zu entwickeln, und gewährleistet insoweit die Interaktion einer Person mit anderen (vgl. Urteil des EGMR [Grosse Kammer] L.B. gegen Ungarn vom 9. März 2023, 36345/16, §§ 102 f.; Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010, 35623/05, §§ 43 f.; BGE 144 I 126 E. 4.1 mit Hinweisen; Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 4.3 mit Hinweisen [nicht publiziert in BGE 149 I 218]). Ein besonders schützenswerter Teil des Privatbereichs ist die Korrespondenz (Art. 8 Ziff. 1 EMRK) beziehungsweise der Brief-, Post- und Fernmeldeverkehr (Art. 13 Abs. 1 BV). Die Konventionsbestimmung ist technikneutral formuliert. Der weite Schutzbereich von Art. 8 Ziff. 1 EMRK umfasst mithin alle (modernen) Formen der Nachrichten- und Datenübermittlung infolge Kommunikation (Urteil des EGMR Michaud gegen Frankreich vom 6. Dezember 2012, 12323/11, § 90; vgl. übereinstimmend für Art. 13 Abs. 1 BV BGE 140 I 353 E. 8.3). Die Kommunikation mit fremden Mitteln gegenüber Drittpersonen soll geheim geführt können; sie soll, wenn sie durch eine Fernmeldedienstanbieterin erfolgt, unter Achtung der Geheimnissphäre vertraulich geführt werden können, ohne dass der Staat Einblick erhält und daraus gewonnene Erkenntnisse gegen die Betroffenen verwendet. Geschützt ist dabei nicht nur der Inhalt der Kommunikation. Der Schutzbereich des Rechts auf Achtung des Privatlebens erfasst in sachlicher Hinsicht auch die sogenannten Randdaten beziehungsweise Verbindungsdaten des Kommunikationsvorgangs. Randdaten sind Daten darüber, wer mit wem, wann, wie lange und von wo aus kommuniziert hat. Auszugehen ist mithin von der Achtung des umfassend zu verstehenden Fernmeldeverkehrs. Die Kommunikation soll vertraulich und vor staatlicher Kenntnisnahme und weiterer Bearbeitung geschützt erfolgen können (vgl. Urteile des EGMR Ekimdzhiev und andere gegen Bulgarien vom 11. Januar 2022, 70078/12, §§ 372 und 376 [unter Verweis auf das zit. Urteil Centrum för rättvisa, §§ 238-244] und Copland gegen Vereinigtes Königreich vom 3. April 2007, 62617/00, § 41-43; BGE 144 I 126 E. 4.1 und E. 6.2; BGE 140 I 353 E. 8.3, je mit Hinweisen). Einen verstärkten Schutz (une protection renforcée) geniesst die Vertraulichkeit der Kommunikation im Verhältnis zwischen Rechtsanwälten und ihren Mandanten; für ein rechtsstaatliches, faires Verfahren ist die Tätigkeit von Rechtsanwälten und damit die Notwendigkeit eines Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant von herausragender Bedeutung. Die Konvention gewährt der Vertraulichkeit der Beziehung zwischen Rechtsanwalt und Mandant insofern einen zusätzlichen Schutz, als der Vertraulichkeit der betreffenden Kommunikation im Rahmen der Beurteilung der Notwendigkeit eines Eingriffs erhöhtes Gewicht zukommt (vgl. zit. Urteil Michaud, §§ 117 ff., insbes. § 118 f.,

bestätigt im Urteil des EGMR Laurent gegen Frankreich vom 24. Mai 2018, 28798/13, §§ 43 f. und 47; auch bereits das Urteil des EGMR Niemietz gegen Deutschland vom 16. Dezember 1992, 13710/88, § 37). In persönlicher Hinsicht erfasst der Schutzbereich alle an der Kommunikation teilnehmenden Personen, das heisst den Absender ebenso wie den Empfänger einer Mitteilung (vgl. Urteil des EGMR Valentino Acatrinei gegen Rumänien vom 25. Juni 2013, 18540/04, §§ 51-53). Befinden sich der Sender und/oder der Empfänger im Ausland, ist für die Frage der Gerichtsbarkeit im Zusammenhang mit der Überwachung der Kommunikation entscheidend, wo die Kommunikation abgefangen, durchsucht und verwendet wird (Urteil des EGMR Wieder und Guarnieri gegen Vereinigtes Königreich vom 12. September 2023, 64371/16 und 64407/16, §§ 87 ff., insbesondere §§ 90-95). Grundrechtsberechtigt sind sodann - soweit hier von Interesse - sowohl natürliche also auch juristische Personen (Urteil des EGMR Telegraaf Media Nederland Landelijke Media B.V. und andere gegen die Niederlande vom 22. November 2012, 39315/06, §§ 7 und 118; vgl. im Ergebnis auch die zit. Urteile Big Brother Watch und andere [Beschwerdeführerin war unter anderem eine Bürgerrechtsorganisation] und Centrum för rättvisa; [Beschwerdeführerin war eine Stiftung]; zudem das Urteil des EGMR Liberty und andere gegen Vereinigtes Königreich vom 1. Juli 2008, 58243/00, § 56 f. [Beschwerdeführerin war unter anderem eine Bürgerrechtsorganisation]; ferner BGE 148 I 226 E. 5.2 mit Hinweisen auf die Rechtsprechung; Schweizer/Striegel, in: St. Galler Kommentar zur Bundesverfassung, 4. Aufl. 2023, Art. 13 Rz. 83 f.; zum örtlichen Geltungsbereich Mark E. Villiger, Handbuch der Europäischen Menschenrechtskonvention [EMRK], 3. Aufl. 2020, Rz. 61 f.).

E. 6.2.2

Die Beschwerdeführenden 4 bis 6 machen sodann geltend, sie seien als Medienschaffende tätig. Sie sehen durch Massnahmen der Funk- und Kabelaufklärung zusätzlich die Medienfreiheit verletzt. Die Bundesverfassung gewährleistet in Art. 17 die Medienfreiheit, das heisst die Freiheit von Presse, Radio und Fernsehen sowie anderer Formen der öffentlichen fernmeldetechnischen Verbreitung von Darbietungen und Informationen. Durch die EMRK wird die Medienfreiheit als Teilgehalt der Freiheit der Meinungsäusserung gemäss Art. 10 Ziff. 1 EMRK geschützt. Die Medienfreiheit enthält in sachlicher Hinsicht eine spezifische Gewährleistung freier öffentlicher, das heisst an einen nicht von Vornherein eingeschränkten Personenkreis adressierter, Äusserungen (BGE 128 IV 53 E. 5c). Sie gehört zu den zentralen Ausprägungen des allgemeinen Grundrechts freier Meinungsäusserung. Normativer Kern der Medienfreiheit ist die Sicherung des ungehinderten Nachrichtenflusses und des freien Meinungsaustauschs. Geschützt ist der gesamte Prozess der Herstellung und Veröffentlichung eines Medienerzeugnisses und somit insbesondere die Recherchetätigkeit des Journalisten, die Herstellung des Medienerzeugnissen und deren Verbreitung beziehungsweise Publikation (BGE 147 I 463 E. 5.3 und BGE 144 I 126 E. 4.1, je mit Hinweisen; Urteil des EGMR Dammann gegen die Schweiz vom 25. April 2006, 77551/01, § 52). Entsprechend schliesst der Schutzbereich der Medienfreiheit in persönlicher Hinsicht alle natürlichen und juristischen Personen ein, die die an der Herstellung und Veröffentlichung eines Medienerzeugnisses beteiligt sind. Die Freiheit des Medienschaffens ist nicht Selbstzweck. Der ungehinderte Fluss von Informationen und Meinungen hat in einem demokratischen Rechtsstaat eine wichtige gesellschaftliche und politische Bedeutung. Insbesondere leisten die Medien einen wesentlichen Beitrag zur Kontrolle behördlicher Tätigkeiten (BGE 141 I 211 E. 3.1 mit Hinweisen; vgl. zudem BGE 143 I 194 E. 3.1 und). Dabei kommt periodisch erscheinenden

Medienprodukten nach der Rechtsprechung des EGMR eine herausgehobene Stellung für die Meinungsbildung zu. Staatliche Eingriffe in diesem Bereich unterliegen daher entsprechend höheren Schranken - bei gleichzeitig höheren Anforderungen an die Berichterstattung (vgl. Robert Esser, in: Löwe-Rosenberg, EMRK, Grosskommentar, Band 12, 27. Aufl. 2024, Art. 10 EMRK Rz. 22 mit Hinweisen, u.a. auf das Urteil des EGMR Ruokanen und andere gegen Finnland vom 6. April 2010, 45130/06, §§ 33 ff.). Unter Umständen kann auch die Tätigkeit von Nichtregierungsorganisationen oder Bloggern in sozialen Netzwerken unter die konventionsrechtlich geschützte Pressefreiheit fallen (vgl. Urteil des EGMR [Grosse Kammer] Magyar Helsinki Bizottság gegen Ungarn vom 8. November 2016, 18030/11, §§ 159, 166 und 168). Anerkannt und in Art. 17 Abs. 3 BV explizit als verfassungsmässiges Recht verankert ist das Recht von Journalisten, Informationsquellen geheim zu halten (Redaktionsgeheimnis). Dieser sogenannte Quellenschutz ist eine Grundvoraussetzung der in einer demokratischen Gesellschaft unerlässlichen Medienfreiheit; ein unzureichender Quellenschutz kann Informanten abschrecken und so die Aufgabe der Medien als «public watchdog» gefährden (zit. Urteil Big Brother Watch und andere, § 442; Urteil des EGMR Jecker gegen die Schweiz vom 6. Oktober 2020, 35449/14, § 33; Urteil des EGMR Voskuil gegen die Niederlande vom 22. November 2007, 64752/01, §§ 64 f.; BGE 151 IV 153 E. 3.2 und E. 3.3.3 f.). Der Schutz journalistischer Quellen schützt - in sachlicher Hinsicht - in erster Linie die Identität von Quellen, schliesst aber auch die Inhalte der betreffenden Angaben und Recherchen mit ein (vgl. Urteil des EGMR [Grosse Kammer] Goodwin gegen Vereinigtes Königreich vom 27. März 1996, 17488/90, § 39, bestätigt mit dem zit. Urteil Big Brother Watch und andere, §§ 442 f.; zit. Urteil Telegraaf Media Nederland Landelijke Media B.V., §§ 125 ff.; BGE 140 IV 108 E. 6.7-6.9). Der Schutzbereich des Quellenschutzes erstreckt sich in persönlicher Hinsicht nicht nur auf Journalisten und alle weiteren Personen, die an der Vorbereitung, Herstellung und Verbreitung von Medienerzeugnissen mitwirken, sondern auch und insbesondere auf die Quelle selbst. Der Umstand, dass die Identität der Quelle den Behörden bekannt ist, hat sodann nicht zur Folge, dass sich der Journalist seinerseits nicht mehr auf den Quellenschutz berufen könnte - auch wenn im Rahmen der Interessenabwägung der Grad des gemäss Art. 10 EMRK gewährten Schutzes unter diesen Umständen nicht mehr dasselbe Gewicht erreichen kann, als wenn die Identität der Quelle geheim gehalten werden soll (vgl. Urteil des EGMR Becker gegen Norwegen vom 5. Oktober 2017, 21272/12, §§ 74-76; BGE 151 IV 153 E. 3.4). Als subsidiäres Auffanggrundrecht zur Medienfreiheit gewährleistet die Meinungsfreiheit das Recht jeder Person, ihre Meinung frei zu bilden und sie ungehindert zu äussern und zu verbreiten (Art. 16 BV; BGE 147 I 463 E. 5.3). Der Schutzbereich umfasst die Gesamtheit der Mitteilungen menschlichen Denkens und alle möglichen Kommunikationsformen (BGE 127 I 145 E. 4b). Die Meinungsfreiheit kann - ebenso wie die weiteren mit ihr in Verbindung stehenden Grundrechte und damit auch die Medienfreiheit - nicht nur durch direkte Eingriffe beeinträchtigt werden, sondern auch mittelbar, wenn der Einzelne aufgrund einer behördlichen Massnahme davon absieht, erneut von seinem Recht Gebrauch zu machen (sog. «chilling effect»; BGE 147 I 372 E. 4.4.2 mit Hinweisen auf die Rechtsprechung; Urteil des BGer 1C_181/2019 vom 29. April 2020 E. 4.2 [nicht publiziert in BGE 147 I 103] mit Hinweis auf BGE 143 I 147 E. 3.2 f.).

E. 6.2.3

Die Beschwerdeführenden rügen weiter, die Funk- und Kabelaufklärung erfolge sogenannt anlasslos, das heisst, es werde ihre Kommunikation überwacht, ohne dass ihr Verhalten

hierzu Anlass gebe. Sie sehen darin eine Verletzung ihres Anspruchs, bis zu einer rechtskräftigen Verurteilung als unschuldig zu gelten (sog. Unschuldsvermutung). Die Unschuldsvermutung ist in Art. 6 Ziff. 2 EMRK und Art. 32 Abs. 1 BV verankert. Sie knüpft an das Schuldstrafrecht an und gewährleistet, als unschuldig behandelt zu werden, bis ein zuständiges Gericht nach Durchführung eines fairen Verfahrens die strafrechtliche Schuld in rechtsgenüglicher Weise nachgewiesen und festgestellt hat. Es ist mithin - als Regel für die Verteilung der Beweislast - Sache der Strafverfolgungsbehörden, dem Beschuldigten seine Täterschaft nachzuweisen (BGE 147 I 57 E. 5.1 und BGE 144 I 126 E. 4.1, je mit Hinweisen). Aus der Unschuldsvermutung und in grundsätzlicher Weise aus dem Anspruch auf ein faires Verfahren folgt unter anderem das sogenannte Selbstbelastungsprivileg («nemo tenetur se ipsum accusare»), das im Strafprozess ein Schweigerecht und ein Recht gewährleistet, nicht zu seiner eigenen Verurteilung beitragen zu müssen (BGE 149 IV 9 E. 5.1.1, BGE 148 IV 205 E. 2.4 und BGE 144 I 126 E. 4.1, je mit Hinweisen; Urteil des BGer 7B_45/2022 vom 21. Juli 2025 E. 2.2.1 mit Hinweisen auf die Rechtsprechung). Das in der EMRK nicht ausdrücklich erwähnte Schweigerecht ist eine wesentliche Ausprägung («au coeur de la notion de procès équitable» bzw. «the heart of the concept of a fair procedure») des in Art. 6 Ziff. 1 EMRK verankerten Anspruchs auf ein faires Verfahren (Urteil des EGMR [Grosse Kammer] John Murray gegen Vereinigtes Königreich vom 8. Februar 1996, 18731/91, § 45; Urteil des EGMR de Légé gegen die Niederlande vom 4. Oktober 2022, 58342/15, § 63). Es bezweckt neben der Gewährleistung eines effektiven Verteidigungsrechts auch - an der Menschenwürde anknüpfend - den Schutz der Willensfreiheit (BGE 147 II 144 E. 5.2.2, BGE 142 IV 207 E. 8.1 und BGE 140 II 384 E. 3.3.4, je mit Hinweisen). Nicht vom sachlichen Geltungsbereich des Selbstbelasungsprivilegs betroffen ist die Verwendung von Daten in einem Strafverfahren, die unabhängig vom Willen der betreffenden Person existieren, das heisst beispielsweise Dokumente, die aufgrund eines Durchsuchungsbefehls beschlagnahmt wurden und von denen die Behörden zuvor Kenntnis hatten (zit. Urteil de Légé, §§ 67 und 76, auch betreffend grundsätzlich unzulässige fishing expeditions). Das Selbstbelastungsprivilegs schützt nicht vor belastenden Äusserungen als solchen, sondern vor der Erlangung von Beweisen durch missbräuchlichen Zwang oder Druck. Zudem gilt das Recht, sich nicht selbst zu belasten, nicht absolut; der ausgeübte Zwang muss ein Ausmass erreichen, das Art. 6 EMRK in seinem Wesensgehalt («substance même» bzw. «very essence of the privilege») beeinträchtigt. Nach der Rechtsprechung des EGMR ist daher jeweils zunächst die Art und das Ausmaß des Zwangs zu prüfen, der zur Erlangung der Beweise ausgeübt wurde. Für die Frage, ob eine Beeinträchtigung vorliegt, sind zudem die vorhandenen Verfahrensgarantien und vor allem die Verwendung der erlangten Informationen massgebend (Urteil des EGMR [Grosse Kammer] Ibrahim und andere gegen Vereinigtes Königreich vom 13. September 2016, 50541/08, 50571/08, 50573/08 und 40351/09, § 269 und zit. Urteil de Légé, § 68 und §§ 74-78). Eine Beeinträchtigung des Selbstbelastungsprivilegs setzt mithin voraus, dass (1) eine Form von Zwang durch die Behörden ausgeübt worden ist und (2) der Zwang auf das Erlangen von Informationen ausgerichtet war, die (alsdann) in einem Strafverfahren verwendet wurden (vgl. zum Ganzen zit. Urteil de Légé, §§ 64-67 und § 74). Der EGMR unterscheidet insbesondere drei Situationen, in denen zu befürchten ist, dass in missbräuchlicher Weise Zwang ausgeübt worden ist (zit. Urteil Ibrahim und andere, § 267): [...] Dans sa jurisprudence, la Cour a distingué au moins trois types de situations de nature à faire craindre l'existence d'une contrainte abusive contraire à l'article 6. La première situation est celle d'un suspect qui,

menacé de subir des sanctions s'il ne témoigne pas, soit témoigne [...]. La deuxième situation est celle où des pressions physiques ou psychologiques, souvent sous la forme de traitements contraires à l'article 3 de la Convention, sont exercées pour obtenir des aveux ou des éléments matériels [...]. La troisième situation est le recours par les autorités à un subterfuge pour extorquer des informations qu'elles n'ont pu obtenir par un interrogatoire [...]. Der persönliche Geltungsbereich der in Art. 6 EMRK und in Art. 32 BV verankerten Verfahrensrechte schliesst zunächst und in erster Linie natürliche Personen ein. Juristische Personen können sich etwa - in differenzierter Anwendung des Selbstbelastungsprivilegs (und) zur Gewährleistung einer wirksamen Verteidigung als Teilgehalt des Anspruchs auf ein faires Verfahren - auf das Selbstbelastungsprivileg berufen (vgl. BGE 147 II 144 E. 5.2, BGE 142 IV 207 E. 8.4, BGE 140 II 384 E. 3.3.4 f. und Urteil des BVGer B-3099/2016, B-3702/2016 vom 17. September 2018 E. 2.2.1 und 4.3, je mit Hinweisen). Die genannten Ansprüche bestehen in sachlicher Hinsicht sodann nur in strafrechtlichen Verfahren. Ob ein auf Erlass einer Sanktion gerichtetes Verfahren eine strafrechtliche Anklage im Sinne von Art. 6 EMRK beinhaltet, bestimmt sich seit der Leitentscheidung «Engel» des EGMR nach den sogenannten Engel-Kriterien. Massgeblich für das Vorliegen einer strafrechtliche Anklage im Sinne von Art. 6 EMRK sind demnach (1) die rechtliche Einordnung des fraglichen Vergehens im nationalen Recht, (2) die Art der Zuwiderhandlung sowie (3) die Art und die schwere der angedrohten Sanktion. Das erste Kriterium bildet dabei im Wesentlichen den für sich alleine nicht entscheidenden Ausgangspunkt der Beurteilung. Die beiden weiteren Kriterien müssen sodann grundsätzlich nur alternativ vorliegen, wobei ein nicht eindeutiges Ergebnis auch eine kumulative Betrachtung erforderlich machen kann (Urteil des EGMR Engel und andere gegen die Niederlande vom 8. Juni 1976, 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, § 82, bestätigt unter anderem mit Urteil des EGMR [Grosse Kammer] Gestur Jónsson und Ragnar Halldór Hall gegen Island vom 22. Dezember 2020, 68273/14 und 68271/14, §§ 75 ff.; vgl. auch BGE 150 I 88 E. 5.2 und BGE 147 I 57 E. 5.2, je mit Hinweisen auf die Rechtsprechung).

E. 6.3.1

Im Folgenden ist zunächst zu prüfen, ob die Funk- und Kabelaufklärung die (sachlichen) Schutzbereiche der als verletzt gerügten Grund- und Konventionsrechte berührt. Der Schutzbereich eines Grundrechts umschreibt dabei, welche Personen im Hinblick auf welche Sachverhalte aus dem Grundrecht welche Ansprüche geltend machen können (Rhinow/Schefer/Uebersax, Schweizerisches Verfassungsrecht, 3. Aufl. 2016, Rz. 1081). Zu klären ist mit anderen Worten im Rahmen einer Konkretisierung der angerufenen Grund- und Konventionsrechte, ob die in Frage stehende Funk- und Kabelaufklärung einen Lebensvorgang betrifft, der durch einen grundrechtlichen Schutzbereich geschützt ist (vgl. zum Vorgehen BGE 142 I 49 E. 5). Gegebenenfalls ist weiter zu prüfen, ob die Funk- und Kabelaufklärung als staatliche Handlung die für eine Grundrechtsbeeinträchtigung erforderliche Intensität aufweist.

E. 6.3.2

Die Beschwerdeführenden machen geltend, bei der Funk- und Kabelaufklärung handle es sich um eine massenhafte und undifferenzierte Überwachung von grenzüberschreitenden Datenströmen, die potentiell auch ihre elektronische Kommunikation betreffe. Schon dies schränke sie in ihrem Kommunikationsverhalten ein: Wer ständig damit rechnen müsse, überwacht zu werden, werde tendenziell von der Möglichkeit, über elektronische Kanäle zu kommunizieren und sich zu informieren, weniger Gebrauch machen (sog. «chilling effect»

bzw. «effet dissuasif»). Im Weiteren beeinträchtigten das Ausleiten und Durchsuchen von Daten durch den Beigeladenen und mehr noch das Speichern und Verwenden von Daten durch die Vorinstanz ihr Privatleben. Dabei müssten die Beschwerdeführenden aufgrund ihrer vielfältigen auch grenzüberschreitenden Kommunikationen und ihres beruflichen und sozialen Engagements in verstärktem Mass damit rechnen, dass ihre Kommunikation vom Beigeladenen und von der Vorinstanz erfasst, gespeichert und bearbeitet werde. Die Vorinstanz trägt mit ihrer Arbeit präventiv zur Sicherheit des Landes bei; ihre Aufgabe ist es insbesondere, sicherheitsrelevante Informationen zu sammeln und zu bearbeiten, um staatsgefährdende Bestrebungen frühzeitig zu erkennen und zu verhindern (vgl. Art. 6 NDG). Die Tätigkeit der Vorinstanz ist insofern klar von der repressiven Tätigkeit der Strafverfolgungsbehörden abzugrenzen (vgl. Botschaft NDG, BBl 2014 2105, 2143). Bei der Funk- und Kabelaufklärung als eine Massnahme zur Informationsbeschaffung handelt es sich um eine präventive und (mithin) anlasslose Überwachung von grenzüberschreitenden Telekommunikationsströmen, die eine massenhafte und praktisch unbegrenzte Erhebung von grenzüberschreitenden Telekommunikationsdaten ermöglicht (sog. Massenüberwachung). Nach der Rechtsprechung des EGMR ist die Massenüberwachung (l'interception en masse bzw. bulk interception) ein schrittweiser Prozess, bei dem die Intensität des Eingriffs in die Ausübung des Rechts auf Achtung des Privatlebens im Laufe des Prozesses zunimmt. Demnach besteht die Massenüberwachung aus vier Phasen. In der ersten Phase wird die elektronische Kommunikation abgefangen und (einschliesslich der Randdaten) gespeichert. Anschliessend wird die gespeicherte Kommunikation einschliesslich der Randdaten (grösstenteils) automatisch durch Anwendung spezifischer Selektoren durchsucht. In einer dritten Phase wird die ausgewählte Kommunikation durch eine Analystin oder einen Analysten überprüft und - in einer vierten Phase - durch die Nachrichtendienste verwendet. Dies kann die Erstellung eines Berichts oder die Weitergabe des Materials an eine andere (auch ausländische) Behörde sein. Nach Auffassung des EGMR greift der Staat in jeder der genannten Phasen in die durch Art. 8 EMRK geschützten Rechte ein; Art. 8 EMRK schützt die Persönlichkeit des Einzelnen umfassend und bereits das blosse Speichern von Daten stellt eine Beeinträchtigung dar. Am Ende des Prozesses, wenn Informationen über eine bestimmte Person von einem Analytiker untersucht und nachrichtendienstlich verwendet werden, ist der Bedarf an Massnahmen zum Schutz vor Missbrauch am grössten (zit. Urteile Big Brother Watch und andere, §§ 324-331 und Centrum för Rättvisa, §§ 239-245; vgl. auch BGE 148 I 233 E. 3.1 f. und BGE 144 I 126 E. 4.1 f. mit Hinweisen). Die Beschwerdeführenden werden vom persönlichen Geltungsbereich des durch die EMRK und die BV geschützten Privatlebens, als dessen Teilgehalt auch die Vertraulichkeit der Kommunikation geschützt ist, erfasst. Dies gilt unstrittig für die natürlichen Personen und - soweit hier von Interesse - auch für den Beschwerdeführer 1 als juristische Person. Auf eine Beeinträchtigung seines Privatbereichs berufen kann sich schliesslich auch der Beschwerdeführer 6, der im Ausland wohnt und seinerseits grenzüberschreitend kommuniziert; der Eingriff in Art. 8 EMRK erfolgt dort, wo die Kommunikation vermutungsweise abgefangen, durchsucht und verwendet wird, das heisst hier in der Schweiz (vgl. vorstehend E. 6.2.1). Wie vorstehend ausgeführt wird sodann im Rahmen der Funk- und Kabelaufklärung jedenfalls ein nicht unerheblicher Teil der grenzüberschreitenden Kommunikation präventiv überwacht. Die Beschwerdeführenden legen glaubhaft dar, dass sie in vielfältiger Weise grenzüberschreitend kommunizieren. Sie müssen mithin damit rechnen, dass auch ihre - vertraulich geführte - Kommunikation zumindest ausgeleitet und automatisiert durchsucht

wird, wobei schon das Erfassen und Durchsuchen von Daten die für eine Grundrechtsbeeinträchtigung nötige minimale Intensität erreicht (vgl. bereits der Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 8.2; zit. Urteil Big Brother Watch und andere, § 330; ferner der Beschluss des deutschen Bundesverfassungsgerichts 1 BvR 1743/16 und 2539/16 vom 8. Oktober 2024, Rz. 141 f. [nachfolgend: Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung]). Die Beschwerdeführenden können insofern nicht mehr uneingeschränkt darauf vertrauen, dass ihre elektronische Kommunikation vertraulich ist. Die Funk- und Kabelaufklärung berühren und beeinträchtigen sie mithin in ihrem Privatleben, das durch Art. 8 EMRK und Art. 13 BV geschützt ist, wobei die Beeinträchtigung an Intensität zunimmt, je weiter der Überwachungsprozess fortschreitet. Zu beachten ist schliesslich, dass die Funk- und Kabelaufklärung auch rein inländische Kommunikation erfasst, soweit diese beispielsweise über Netzwerke und Server im Ausland erfolgt (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 6.2.2; zudem der zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Ziff. 142). Auch in dieser Hinsicht ist mithin der Schutzbereich von Art. 8 EMRK und Art. 13 BV berührt und beeinträchtigt der Staat mit der Funk- und Kabelaufklärung das Privatleben der Beschwerdeführenden 1 bis 5 und 7; in welchem Mass die Funk- und Kabelaufklärung auch inländische Kommunikation erfasst, ist an dieser Stelle noch nicht von Bedeutung (vgl. hierzu nachfolgend E. 11.4). Der berührte und beeinträchtige Anspruch auf Achtung des Privatlebens stellt eine spezifische Konkretisierung des umfassenden Rechts auf selbstbestimmte Entfaltung der Persönlichkeit dar (vgl. Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 4.3 mit Hinweisen [nicht publiziert in BGE 149 I 218]). Dem verfassungsmässigen Anspruch auf persönliche Freiheit und Bewegungsfreiheit (Art. 10 Abs. 2 BV) kommt daher hier keine weitergehende gehende Bedeutung zu. Dies gilt im Ergebnis auch für die von den Beschwerdeführenden ebenfalls angerufenen Versammlungsfreiheit (Art. 11 EMRK; Art. 22 BV); die individuelle Kommunikation im Hinblick etwa auf die Organisation und Durchführung einer Versammlung fällt in den Schutzbereich des Privatlebens und ist mithin durch Art. 8 EMRK und Art. 13 Abs. 1 BV geschützt.

E. 6.3.3

In einem nächsten Schritt ist zu prüfen, ob auch der Schutzbereich der Medienfreiheit durch Massnahmen der Funk- und Kabelaufklärung berührt ist. Gemäss der Beschwerdeschrift vom 30. Oktober 2017 sind die Beschwerdeführenden 4, 5 und 6 als Medienschaffende insbesondere im Bereich des investigativen Journalismus zu internationalen Themen tätig. Entsprechend würden sie in vielfältiger Weise elektronische Kommunikationsmittel nutzen sowie grenzüberschreitend kommunizieren und seien insbesondere zum Schutz ihrer Quellen auf eine vertrauliche Kommunikation angewiesen. Dies erscheint jedenfalls für die Beschwerdeführerin 4 und den Beschwerdeführer 6 im Urteilszeitpunkt glaubhaft dargelegt. Sie fallen mithin in den persönlichen Schutzbereich der Medienfreiheit. Der Beschwerdeführer 1 ist ein Verein für Bürger- und Konsumentenschutz insbesondere hinsichtlich der Nutzung von digitalen Netzen, Medien und Inhalten. Zu diesem Zweck veröffentlicht der Verein unter anderem Publikationen auf seiner Homepage (...). Ob es sich dabei um Medienerzeugnisse im vorerwähnten Sinn handelt und mithin auch der Beschwerdeführer 1 in den persönlichen Schutzbereich der grundrechtlich geschützten Medienfreiheit (Art. 17 BV, Art. 10 Ziff. 1 EMRK) fällt, kann offen bleiben, da im Rahmen der gesamthaft vorzunehmenden Beurteilung jedenfalls mit Blick auf die

Beschwerdeführenden 4 und 6 ohnehin davon auszugehen ist, dass der persönliche Schutzbereich der Medienfreiheit berührt ist. Den sachlichen Schutzbereich betreffend ging der EGMR im zitierten Urteil Big Brother Watch und andere davon aus, dass der Staat durch die Massenüberwachung in den Schutzbereich der Medienfreiheit eingreift: Selbst wenn die verwendeten Selektoren beziehungsweise Suchbegriffe nicht so beschaffen seien beziehungsweise sein dürften, dass die Auswahl von vertraulichem journalistischem Material sehr wahrscheinlich sei, bestehe das Risiko, dass entsprechendes Material als Beifang einer Massenüberwachung gespeichert und analysiert werde. Die Analyse könne dazu führen, dass eine Quelle identifiziert werde, weshalb solide Schutzvorkehren bereits in Bezug auf die Speicherung und Untersuchung von solch vertraulichem Material erforderlich seien (zit. Urteil Big Brother Watch und andere, §§ 449 f.). Auch bei der hier streitigen Funk- und Kabelaufklärung besteht die Gefahr, dass journalistisches Material gespeichert, durchsucht und analysiert wird, umso mehr, als etwa Angaben über Journalisten im Ausland als Suchbegriff nicht ausgeschlossen sind (Art. 39 Abs. 3 NDG e contrario; vgl. auch Erläuternder Bericht Revision NDG zu Art. 39). Es besteht mithin die Möglichkeit, dass den Behörden im Rahmen der Funk- und Kabelaufklärung Quellen der journalistisch tätigen Beschwerdeführenden bekannt werden. Bereits die Gefahr des Bekanntwerdens einer Quelle kann zudem abschreckende beziehungsweise einschüchternde Wirkung haben, weil Journalisten und deren Quellen nicht mehr auf die Vertraulichkeit ihrer elektronischen Kommunikation vertrauen («chilling effect»; vgl. vorstehend E. 6.2.2). Die für eine Grundrechtsbeeinträchtigung erforderliche Intensität ist unter diesen Umständen und mit Blick auf das zit. Urteil Big Brother Watch und andere erreicht. Gleich wie im Zusammenhang mit dem Anspruch auf Achtung des Privatlebens können jedenfalls die als Medienschaffende tätigen Beschwerdeführenden 4 und 6 nicht mehr auf die Vertraulichkeit ihrer elektronischen Kommunikation vertrauen, womit die Funk- und Kabelaufklärung sie in ihrer Medienfreiheit gemäss Art. 10 EMRK und Art. 17 BV berührt und beeinträchtigt. In welchem Mass die Medienfreiheit und damit verbunden der Quellenschutz beeinträchtigt ist und welche Schutzvorkehren das anwendbare Recht vorsieht, ist an dieser Stelle nicht von Bedeutung; ob das anwendbare Recht hinreichende Schutzvorkehren vorsieht, wird im Rahmen der Rechtfertigung der Beeinträchtigung zu beurteilen sein. Im Verhältnis zur grundrechtlich geschützten Meinungsfreiheit (Art. 16 BV; vgl. auch Art. 19 UNO-Pakt II) besteht hier keine echte Konkurrenz; für die Beschwerdeführenden 1 sowie 4, 5 und 6 konkretisiert die Medienfreiheit die berufsspezifischen grundrechtsgeschützten Ansprüche und die Meinungsfreiheit gewährt in dieser Hinsicht keine weitergehenden Ansprüche (BGE 144 I 126 E. 4.2 mit Hinweis auf BGE 137 I 209 E. 4.2; vgl. auch BGE 137 I 167 E. 3.7). Die individuelle Kommunikation (mit fremden Mitteln) wird zudem, wie vorstehend ausgeführt, durch Art. 13 Abs. 1 BV (Schutz der Privatsphäre) geschützt, weshalb sich aus der Meinungsfreiheit gemäss Art. 16 BV auch in Bezug auf die weiteren privaten Beschwerdeführenden keine weitergehenden Ansprüche ergeben.

E. 6.3.4

Die Beschwerdeführenden machen sodann geltend, Massnahmen der Funk- und Kabelaufklärung berührten sie in der grundrechtlich geschützten Unschuldsvermutung. Nach dieser gelte jeder Mensch als unschuldig, so lange er nicht in einem rechtmässig geführten Verfahren für schuldig befunden worden sei. Zudem habe die beschuldigte Person in einem solchen Verfahren das Recht auf Aussageverweigerung als Teilgehalt des Selbstbelastungsprivilegs; sie müsse sich nicht selbst belasten. Beides sei im Rahmen der

anlasslosen Überwachung auch ihrer Kommunikation im Rahmen von Massnahmen der Funk- und Kabelaufklärung nicht gewährleistet. Die Vorinstanz beeinträchtige daher zusätzlich ihre Unschuldsvermutung und das Selbstbelastungsprivileg gemäss Art. 6 Ziffn. 1 und 2 EMRK sowie Art. 32 Abs. 1 und 2 BV. Der sachliche Schutzbereich von Art. 6 EMRK und Art. 32 BV ist, soweit im Zusammenhang mit der Unschuldsvermutung und dem Selbstbelastungsprivileg von Interesse, auf strafrechtliche Verfahren beschränkt, Verfahren also, die repressiv auf Erlass einer Sanktion gerichtet sind und mithin einen strafrechtlichen Charakter haben (vgl. vorstehend E. 6.2.3). Das Bundesgericht hat sich mit Blick auf den Schutzbereich von Art. 6 EMRK und Art. 32 BV bereits mehrfach mit der Frage befasst, ob beziehungsweise unter welchen Umständen Beschaffung beziehungsweise Speicherung und Aufgebwahrung von Personendaten das grundrechtlich geschützte Selbstbelastungsprivileg beziehungsweise die Unschuldsvermutung beeinträchtigen. Es hielt etwa fest, mit der nicht geheimen Speicherung von Randdaten der Kommunikation werde kein gegen das Selbstbelastungsprivileg verstossender Zwang ausgeübt. Zudem könne aus der Speicherung und Aufbewahrung von Personendaten ausserhalb eines Strafverfahrens nicht ohne Weiteres eine Verdachtsäusserung oder der Vorwurf einer Schuld im strafrechtlichen Sinn abgeleitet werden (BGE 144 I 126 E. 4.1 f. betreffend Randdaten der Telekommunikation und BGE 138 I 256 E. 4 betreffend die Speicherung von Daten in einem polizeilichen Informationssystem, je mit Hinweisen; vgl. auch Urteil des BGer 1C_51/2008 vom 30. September 2008 E. 3.2 mit Hinweisen). Entsprechendes erkennt - hinsichtlich der Unschuldsvermutung - grundsätzlich auch der EGMR (Urteil des EGMR M.K. gegen Frankreich vom 18. April 2013, 19522/09, § 36 mit Hinweis auf das Urteil des EGMR [Grosse Kammer] S. und Marper gegen Vereinigtes Königreich vom 4. Dezember 2008, 30562/04, 30566/04, § 122). Die Vorinstanz trägt präventiv zur Sicherheit der Schweiz bei (vgl. Art. 6 Abs. 1 NDG). Die hier mit der Funk- und Kabelaufklärung in Frage stehende sicherheitspolizeiliche Tätigkeit der Vorinstanz ist insofern von der repressiven Tätigkeit der Strafverfolgungsbehörden abzugrenzen; die Vorinstanz nimmt unmittelbar keine repressiven polizeilichen oder strafprozessualen Aufgaben war (Botschaft NDG, BBl 2014 2105, 2143). Aus der vermuteten Bearbeitung von Personendaten der Beschwerdeführenden durch den Beigeladenen und die Vorinstanz lässt sich daher für sich allein weder ein Verdacht noch eine Schuld im strafprozessualen beziehungsweise strafrechtlichen Sinn ableiten. Zudem ist nicht ersichtlich und wird auch nicht begründet geltend gemacht, durch die Bedingungen für die Speicherung der Daten durch die Vorinstanz oder die Art der Aufbewahrung entstehe der Eindruck, die Beschwerdeführenden würden nicht als unschuldig gelten (vgl. zit. Urteil M.K., § 36; ferner das zit. Urteil S. und Marper, §§ 122 und 125). Grundsätzlich ist daher der Schutzbereich von Art. 6 Ziff. 2 EMRK und Art. 32 Abs. 1 BV durch Massnahmen der Funk- und Kabelaufklärung nicht berührt. Zwischen der Vorinstanz und den Strafverfolgungsbehörden besteht jedoch eine Schnittstelle: Dienen Erkenntnisse der Vorinstanz anderen Behörden zur Strafverfolgung, so stellt die Vorinstanz ihnen diese gemäss Art. 60 Abs. 2 NDG unaufgefordert oder auf Anfrage hin zur Verfügung. Daten aus genehmigungspflichtigen Beschaffungsmassnahmen gibt die Vorinstanz immer dann einer Strafverfolgungsbehörde bekannt, wenn sie konkrete Anhaltspunkte für eine Straftat enthalten, zu deren Verfolgung die Strafverfolgungsbehörde eine vergleichbare strafprozessuale Massnahme anordnen dürfte (Art. 60 Abs. 3 NDG). Die Schnittstelle zwischen der Vorinstanz und den Strafverfolgungsbehörden ist, wie nachfolgend zu zeigen sein wird, insbesondere mit Blick auf den Grundsatz nemo tenetur se ipsum accusare, wie er in Art. 32 Abs. 2 BV und Art. 6

Ziff. 1 EMRK gewährleistet wird, nicht von vornherein ohne Relevanz. Im Strafprozess kommt dem Tatverdacht grundlegende Bedeutung zu. Bereits ein polizeiliches Vorverfahren setzt einen Tatverdacht voraus (Art. 299 Abs. 2 der Strafprozessordnung [StPO, SR 312.0]). Im weiteren Verlauf löst der hinreichende Tatverdacht den Widerspruch auf zwischen der Unschuldsvermutung und dem Einsatz von Zwangsmassnahmen (Art. 197 Abs. 1 Bst. b StPO). Der Tatverdacht begründet in diesem Sinne das öffentliche Interesse an der Strafverfolgung und dem mit Zwangsmassnahmen verbundenen Grundrechtseingriff (Art. 36 Abs. 2 BV). In diesem Sinne kommt dem Tatverdacht eine die Strafverfolgung legitimierende und (damit) rechtsstaatlich-limitierende Funktion zu. Demgegenüber ist im Bereich der präventiven Tätigkeit der Vorinstanz etwa eine Bedrohung der inneren Sicherheit nicht - wie im Strafprozess - Anlass für eine nachrichtendienstliche Informationsbeschaffung. Vielmehr hat die Informationsbeschaffung umgekehrt die Suche nach möglichen Bedrohungen zum Ziel. Dies gilt in besonderem Mass für die Funk- und die Kabelaufklärung. Bei ihnen handelt es sich um Mittel der anlasslosen Massenüberwachung. Ermittlungen ohne Tatverdacht, sogenannte fishing expeditions beziehungsweise Beweisausforschungen, sind nicht nur möglich, sondern geradezu geboten, wohingegen die Ergebnisse solcher Beweisausforschungen im Strafprozess grundsätzlich nicht verwertet werden dürften (vgl. Gfeller/Thormann, in: Basler Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl. 2023, Art. 243 Rz. 15 ff. und 39 ff.; Elena Biaggini, Verwertbarkeit verdachtsbegründender Informationen aus Fernmeldeüberwachungen im Strafverfahren, 2022, Rz. 247 f., 254 ff., 264, 267 ff.; Wolfgang Wohlers, Die Verwertbarkeit staatlich erstellter Videoaufzeichnungen im Strafprozess, Schweizerische Zeitschrift für Strafrecht [ZStrR] 2022 S. 64 f.; Isenring/Quiblier, Der Preis der Sicherheit, in: Sicherheit & Recht 2017 S. 131; Ackermann/Vogler, Nachrichtendienst und Strafprozess - zur Verwertbarkeit von Beweisen zwischen Systemen, in: Ackermann/Hilf [Hrsg.], TOP SECRET, Geheimnisschutz und Spionage, 8. Schweizerische Tagung zum Wirtschaftsstrafrecht, 2015, S. 164 f., 166 und 169; Patrick von Hahn, Nr. 21 Bundesgericht, Strafrechtliche Abteilung, Urteil vom 27. Januar 2016 i.S. A.X. und B.X. gegen Schweizerische Bundesanwaltschaft - 6B_57/2015, 6B_81/2015, forumpoenale 2016 S. 149 f.; zur unzulässigen Beweisausforschung BGE 149 IV 369 E. 1.3.1 mit Hinweisen). Mit Blick auf die Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an die Strafverfolgungsbehörden fällt besonders der folgende Aspekt ins Gewicht: Das Nachrichtendienstgesetz unterscheidet im 3. Kapitel zur Informationsbeschaffung unter anderem zwischen genehmigungsfreien Beschaffungsmassnahmen (1. Abschnitt; Art. 13 ff. NDG), genehmigungspflichtigen Beschaffungsmassnahmen (4. Abschnitt; Art. 26 ff. NDG) und der Informationsbeschaffung im Ausland (6. und 7. Abschnitt; Art. 36 ff. und Art. 39 ff. NDG). Die Funk- und die Kabelaufklärung (Art. 38 und Art. 39 ff. NDG), die hier in Frage stehen, dienen der Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland (vgl. auch den zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Rz. 97, wonach die der Kabelaufklärung vergleichbare «strategische Überwachung» beziehungsweise «strategische Telekommunikationsüberwachung» aufgrund ihrer Anlasslosigkeit nur als Instrument der Auslandsaufklärung eingesetzt werden darf). Es handelt sich bei der Funk- und der Kabelaufklärung nicht um «genehmigungspflichtige Beschaffungsmassnahmen» im Sinne des 4. Abschnitts zum 3. Kapitel des NDG (Botschaft NDG, BBl 2014 2105, 2107 und 2178). Der Grund hierfür ist, dass die Informationsbeschaffung im Ausland in der Regel als Spionage beurteilt wird. Zudem verfügen Schweizer Behörden im Ausland über keine

Hoheitsbefugnisse, so dass Erkenntnisse in der Regel nicht unmittelbar zu Folgemassnahmen für die Betroffenen führen. Es wurde aus diesen Gründen darauf verzichtet, die Massnahmen zur Informationsbeschaffung im Ausland als genehmigungspflichtige Beschaffungsmassnahmen auszugestalten (Botschaft NDG, BBl 2014 2105, 2174 f.; vgl. auch das Urteil des deutschen Bundesverfassungsgerichts 1BvR 2835/17, Rz. 149 und 165 [nachfolgend: Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung]). Daran, dass es sich bei der Kabelaufklärung nicht um eine sogenannt genehmigungspflichtige Beschaffungsmassnahme im Sinne von Art. 26 ff. NDG handelt, ändert nichts, dass Anträge zur Kabelaufklärung genehmigungspflichtig sind (Art. 40 Abs. 1 NDG); die Genehmigungspflicht besteht, weil die Kabelaufklärung nur mit der Beteiligung schweizerischer Anbieterinnen von Fernmeldediensten durchgeführt werden kann und diesen eine rechtsgültige Anordnung für das Aus- beziehungsweise Weiterleiten der betreffenden Datenströme an die Beigeladene übergeben werden können muss. Diese Genehmigungspflicht führt aber nicht zu einer Qualifikation der Kabelaufklärung als sogenannt genehmigungspflichtige Beschaffungsmassnahme im Sinne des Nachrichtendienstgesetzes (Botschaft NDG, BBl 2014 2105, 2178). Bei der Funk- und Kabelaufklärung handelt es sich nach dem Gesagten nicht um genehmigungspflichtige Beschaffungsmassnahmen im Sinne des Nachrichtendienstgesetzes. Erkenntnisse der Vorinstanz aus der Funk- und Kabelaufklärung dürfen mithin den Strafverfolgungsbehörden bekannt gegeben werden (Art. 60 Abs. 2 NDG), ohne dass die Hürden von Art. 60 Abs. 3 NDG zur Anwendung kommen, die für die Bekanntgabe von Daten aus genehmigungspflichtigen Beschaffungsmassnahmen im Sinne von Art. 26 ff. NDG gelten (vgl. auch Botschaft NDG, BBl 2014 2105, 2193 f.). Gleichwertige Massnahmen zum Schutz vor Missbrauch lassen sich Art. 60 Abs. 2 NDG nicht (ohne Weiteres) entnehmen. Vielmehr reicht es für eine Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an die Strafverfolgungsbehörden aus, dass diese der Strafverfolgung «dienen». Zudem fällt an dieser Stelle in Betracht, dass der Beigeladene gemäss Art. 39 Abs. 4 Bst. b und Abs. 5 sowie Art. 42 Abs. 2 und 3 NDG Daten und Erkenntnisse über Personen im Inland, die sie im Rahmen einer Funk- oder Kabelaufklärung gewonnen hat, unverändert - das heisst nicht anonymisiert - an die Vorinstanz weiterleitet, wenn die Daten Informationen über Vorgänge im In- oder Ausland enthalten, die auf eine konkrete Bedrohung der inneren Sicherheit gemäss Art. 6 Abs. 1 Bst. a NDG hinweisen. Die Zweckrichtung der Funk- und Kabelaufklärung als Instrumente zur Informationsbeschaffung über Vorgänge im Ausland bildet mithin keine unüberwindbare Hürde mit Blick auf die Informationsbeschaffung über Personen im Inland und die Bekanntgabe von Erkenntnissen an die Strafverfolgungsbehörden. Die Bekanntgabe von Informationen erfolgt schliesslich durch sogenanntes informelles Verwaltungshandeln, ohne dass Betroffene darüber in Kenntnis gesetzt würden. Eine unmittelbare Rechtsschutzmöglichkeit besteht nicht (vgl. für die im Bereich des Finanzmarktrechts vergleichbare Situation das Urteil des BVGer A-4640/2022 vom 13. März 2025 E. 3.5). Vor diesem Hintergrund fragt sich, ob die - soweit hier von Interesse - übliche Umschreibung und Eingrenzung des Schutzbereichs von Art. 6 EMRK auf Strafverfahren beziehungsweise dessen Umschreibung anhand der sogenannten Engel-Kriterien (vgl. hierzu vorstehend E. 6.2.3) der Bedeutung der Schnittstelle zwischen präventiver nachrichtendienstlicher Tätigkeit und repressiver Strafverfolgung hinreichend Rechnung zu tragen vermag. Diese Frage drängt sich insbesondere mit Blick auf den effektiv zu gewährleistenden Grundrechtsschutz auf. Vor diesem Hintergrund wäre zu

prüfen, ob und inwieweit die präventive Informationsbeschaffung der Vorinstanz im Rahmen der Funk- und Kabelaufklärung jedenfalls in Bezug auf Personen im Inland nicht gleichzeitig auch strafprozessualer Natur ist und mithin im Hinblick auf die Möglichkeit einer Verwendung von nachrichtendienstlichen Erkenntnissen zur Strafverfolgung die im Strafprozess geltenden, durch Verfassung und EMRK garantierten Grundsätze Anwendung finden müssten. Dabei setzt der sachliche Anwendungsbereich des Rechts, sich nicht selbst zu belasten (Selbstbelastungsprivileg), voraus, dass die Behörde Zwang ausübt (vgl. vorstehend E. 6.2.3). Ein solcher Zwang könnte darin bestehen, auf elektronische Telekommunikation und damit - in der heutigen Zeit - grundsätzlich auf Telekommunikation überhaupt zu verzichten, um nicht Gefahr zu laufen, dass eigene Personendaten in einem Strafprozess verwendet werden. Die Rechtsprechung hat sich in anderem Zusammenhang bereits mit der Frage befasst, ob und inwieweit etwa das Selbstbelastungsprivileg ausserhalb des Strafprozesses Wirkung entfaltet. So hielt das Bundesgericht betreffend die Finanzmarktaufsicht und ein im Anschluss an das aufsichtsrechtliche Verfahren geführtes Verwaltungsstrafverfahren fest (Urteil des BGer 6B_1355/2020 vom 14. Januar 2022 E. 3.3): Das vorliegende Strafverfahren richtet sich nach dem VStrR (vgl. Art. 1 VStrR i.V.m. Art. 1 Abs. 1 lit. d und Art. 50 Abs. 1 des Bundesgesetzes vom 22. Juni 2007 über die Eidgenössische Finanzmarktaufsicht [Finanzmarktaufsichtsgesetz, FINMAG; SR 956.1]). Gemäss Art. 77 Abs. 4 VStrR sind rechtskräftige Entscheide von verwaltungsunabhängigen Rechtspflegeinstanzen über die Leistungs- oder Rückleistungspflicht für das Strafgericht verbindlich (vgl. BGE 111 IV 189 E. 3). Art. 77 Abs. 4 VStrR ist rechtsstaatlich bedenklich, weil die Beweisführung und Sachverhaltsfeststellung damit im Verwaltungsverfahren erfolgt, das den Anforderungen von Art. 6 EMRK nicht genügt. [...] Das Bundesgericht erachtete im zitierten Urteil die erhobenen Beweismittel als auch im Strafverfahren verwertbar, da im zu beurteilenden Fall die Beweiserhebung im Verwaltungsverfahren unter Beachtung der Anforderungen von Art. 6 EMRK beziehungsweise der im Strafprozess geltenden Grundsätze erfolgt war (Urteil des BGer 6B_1355/2020 vom 14. Januar 2022 E. 3.3; vgl. ebenfalls in diesem Sinn das Urteil des Bundesstrafgerichts CA.2020.10 vom 2. August 2021 E. 2.1.5, insbes. E. 2.1.5.5 ff.; ferner das Urteil des BVGer B-3099/2016 vom 17. September 2018 E. 1.5.6, wonach das Verbot des Selbstbelastungszwangs nicht auf ein reines Verwertungsverbot reduziert werden darf). In einem jüngeren Entscheid in gleichem Sachzusammenhang kam das Bundesgericht zum Ergebnis, dass die im Verwaltungsverfahren erlangten Kenntnisse im Strafprozess nicht hätten verwendet werden dürfen; im Verwaltungsverfahren war der Hinweis unterblieben, dass der Betroffene seine Mitwirkung hätte verweigern dürfen (Urteil des BGer 7B_45/2022 vom 21. Juli 2025 E. 2). Auch in anderem Zusammenhang, etwa in Bezug auf die Verwertung von Erkenntnissen, welche der Nachrichtendienst oder die Polizei im Rahmen ihrer präventiven Tätigkeit erlangt haben, hat sich das Bundesgericht mit der Frage zu befassen gehabt, wie mit den betreffenden Erkenntnissen im anschliessenden Strafverfahren umzugehen ist. Es hat seine Beurteilung dabei im Wesentlichen auf die Frage der Verwertbarkeit beschränkt und hierbei auf die hinter der Regelung von Art. 141 Abs. 2 StPO stehende Wertung - die Verwertung rechtswidrig erlangter Beweise unter gewissen Umständen zuzulassen - abgestellt (BGE 146 I 11 E. 4.3; vgl. zudem das Urteil des BGer 6B_57/2015 vom 27. Januar 2016 E. 3.2.1). Auch in der Lehre werden die Fragen, die sich im Zusammenhang mit der Schnittstelle zwischen präventiver behördlicher Tätigkeit und repressiven strafprozessualen Handlungen stellen, im Wesentlichen unter dem Titel der Verwertbarkeit von ausserhalb des Strafprozesses

erlangten Beweismitteln diskutiert. Es wird darauf hingewiesen, dass die Verwendung beispielsweise nachrichtendienstlich erlangter Informationen im Strafprozess eine Abkehr vom Paradigma des Beweismittels als Ergebnis verdachtsgesteuerter Ermittlungshandlungen darstellt. Es seien daher Schranken für die strafprozessuale Verwertung zu definieren, die eine Vorverlagerung des Strafverfahrens in die präventive polizeiliche oder nachrichtendienstliche Tätigkeit verhindern. Dabei lassen sich im Wesentlichen drei verschiedene Begründungsansätze unterteilen (vgl. die Übersicht bei E. Biaggini, a.a.O., Rz. 278 ff.). Gemäss einem ersten Ansatz (1) sind nachrichtendienstliche Erkenntnisse im Strafprozess absolut unverwertbar. Andere Autoren (2) erachten die Bekanntgabe und Verwertung nachrichtendienstlicher Erkenntnisse (unter unterschiedlichen Titeln) im Strafprozess mit Blick auf die hinter Art. 60 Abs. 2 und 3 NDG stehende Wertung - die Bekanntgabe von Daten an die Strafverfolgungsbehörden im Grundsatz zuzulassen - sowie unter dem Vorbehalt entgegenstehender Interessen als grundsätzlich zulässig. Schliesslich (3) wird für die Frage der Verwertbarkeit teilweise darauf abgestellt, ob seitens der Strafverfolgungsbehörden - vergleichbar der Beurteilung der Verwertbarkeit von Beweisen, die durch Private rechtswidrig beschafft worden sind - eine hypothetische rechtmässige Erhebungsmöglichkeit (gestützt auf eine abstrakte Hypothesenbildung) besteht und die Verwendung präventiv erlangter Beweise zum Zweck der Strafverfolgung im Einzelfall verhältnismässig ist (vgl. zum Ganzen Sabine Gless, in: Basler Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl. 2023, Art. 141 Rz. 38b; Wohlers, a.a.O., S. 55 f. und 61 f.; E. Biaggini, a.a.O., Rz. 278 ff., 306 ff., 376 ff. und 519 ff.; Hansjakob/Pajarola, in: Donatsch/Lieber/Summers/Wohlers [Hrsg.], Kommentar zur Schweizerischen Strafprozessordnung StPO, 3. Aufl. 2020, Art. 278 StPO Rz. 130-133; Jan Hecker, Allgemeine Verfassungsfragen der Nachrichtendienste, in: Dietrich/Eiffler [Hrsg.], Handbuch des Rechts der Nachrichtendienste, 2017, III § 2 Rz. 37-40; Isenring/Quiblier, a.a.O., S. 131; von Hahn, a.a.O., S. 149 f.; Ackermann/Vogler, a.a.O., S. 178 ff.; vgl. zur Verwertbarkeit von Beweisen, die durch Private rechtswidrig beschafft worden sind BGE 151 IV 124). Für die hier zu beurteilende Frage, ob die vermutete Bearbeitung von Personendaten der Beschwerdeführenden durch die Vorinstanz den sachlichen Schutzbereich von Art. 6 (Ziff. 1) EMRK und Art. 32 (Abs. 2) BV berührt, ist das Folgende festzuhalten: Die Bekanntgabe von Erkenntnissen der Vorinstanz an die Strafverfolgungsbehörden ist zunächst einmal - im datenschutzrechtlichen Sinn - eine Bearbeitung von Personendaten (vgl. Art. 5 Bst. d DSG). Zudem ist die Bekanntgabe mit einer Zweckänderung verbunden. Beides, Bekanntgabe und Zweckänderung, ist je ein eigenständiger Eingriff in den Privatbereich, der durch Art. 8 EMRK und Art. 13 BV geschützt ist. Dabei ist die Änderung von einer klar zugewiesenen präventiven hin zu einer repressiven Zweckausrichtung in besonderem Mass rechtfertigungsbedürftig. Der Grundsatz der Zweckbindung (Art. 6 Abs. 3 DSG) umfasst zwei Komponenten. Zunächst bedarf jede Datenerhebung einer hinreichend bestimmten Zweckbestimmung. Die erhobenen Daten sind alsdann im Sinne einer Zweckbindung an den vorgängig bestimmten Zweck gebunden. Eine Zweckänderung verlangt mithin nach einer gesetzlichen Grundlage für die Datenbearbeitung im Lichte des neuen Verwendungszwecks. Zudem muss der neue Verwendungszweck einem öffentlichen Interesse entsprechen und verhältnismässig sein (Art. 36 Abs. 2 und Abs. 3 BV). Der grundrechtlich verankerte Anspruch auf Achtung des Privatbereichs (Art. 8 EMRK; Art. 13 BV) hat hier insofern auch eine spezifisch strafprozessuale Dimension, als sich daraus Vorgaben für die Verwendung von Informationen im Strafprozess ergeben. Konkret beschränkt der Grundsatz der

Zweckbindung die Verwendung von nachrichtendienstlich gewonnenen Informationen im Strafprozess: Die Strafverfolgungsbehörden dürfen Informationen grundsätzlich nur gestützt auf eine hinreichende Ermächtigungsgrundlage verwenden (vgl. in diesem Sinne E. Biaggini, a.a.O., Rz. 266, 301 und insbes. 359 ff.; ferner Wohlers, a.a.O., S. 62, 64 und 71 ff.; Zimmerlin/Galella, Aspekte der beweismässigen Verwertbarkeit von polizeilichen Informationen im Strafverfahren, forumpoenale 2019 S. 376 und 379; Ackermann/Vogler, a.a.O., S. 174 ff.; ferner beispielsweise Art. 273 StPO, der für die Überwachung des Post- und Fernmeldeverkehrs - in generell-abstrakter Abwägung mit dem grundrechtlichen Anspruch auf Achtung des Fernmeldeverkehrs - einen dringenden Tatverdacht in Bezug auf eine Straftat von hinreichender Schwere und somit ein gewichtiges öffentliches Interesse verlangt). Gegenstand des vorliegenden Beschwerdeverfahrens ist die vermutete Bearbeitung der Personendaten der Beschwerdeführenden durch die Vorinstanz - und damit verbunden die mögliche Bekanntgabe von Erkenntnissen an die Strafverfolgungsbehörden. Eine (konkrete) strafprozessuale Verwertung von Erkenntnissen steht nicht in Frage. Ausgangspunkt für die nachstehende materielle Beurteilung ist somit der verfassungsrechtliche Datenschutz beziehungsweise der in EMRK und Bundesverfassung geschützte Privatbereich und als Teilbereich dessen der Anspruch auf informationelle Selbstbestimmung (vgl. in diesem Sinne auch E. Biaggini, a.a.O., Rz. 301, 371, 466). Zu beurteilen wird sein, ob für die Übermittlung von Erkenntnissen der Vorinstanz an die Strafverfolgungsbehörden und für die damit verbundene Zweckänderung eine hinreichende gesetzliche Grundlage besteht und diese hinreichenden und wirksamen Schutz vor Missbrauch vorsieht. Hierbei wird auch die neue Zweckrichtung der bekannt gegebenen Erkenntnisse - die Verwendung zur Strafverfolgung - zu berücksichtigen sein (vgl. hierzu nachfolgend E. 16.3.4.3). Nicht Gegenstand der Beurteilung ist hingegen die Zulässigkeit beziehungsweise Verhältnismässigkeit der Verwendung von Erkenntnissen der Vorinstanz aus der Funk- und Kabelaufklärung im Strafprozess; die Frage der Verwertbarkeit solcher Erkenntnisse ist im Einzelfall im anschliessenden Verfahren, das heisst im konkreten Strafprozess selbst, zu prüfen (vgl. in diesem Sinne Urteile des BGer 7B_45/2022 vom 21. Juli 2025 E. 2.2.4 mit Hinweisen und 1B_268/2019 vom 25. November 2019 E. 2.2 f.; Urteil des BVGer B-4763/2017 vom 29. Juni 2018 E. 3.4). Für das vorliegende Beschwerdeverfahren ist somit davon auszugehen, dass die mögliche Bekanntgabe von Erkenntnissen an die Strafverfolgungsbehörden eine weitere Beeinträchtigung des Privatbereichs (Art. 8 EMRK, Art. 13 BV) der Beschwerdeführenden darstellt. Hingegen ist im vorliegenden Kontext nicht davon auszugehen, dass der Schutzbereich von Art. 6 EMRK und von Art. 32 BV berührt ist (vgl. im Ergebnis auch das Urteil des EGMR Weber und Saravia gegen Deutschland vom 29. Juni 2006, 54934/00, § 79; ferner das zit. Urteil S. und Marper, §§ 122 und 125 f.).

E. 6.4

Geheime Überwachungsmassnahmen wie hier die Funk- und die Kabelaufklärung können auch die Verfahrensgrundrechte beeinträchtigen, allen voran den Anspruch auf rechtliches Gehör (Art. 29 Abs. 2 BV) und das in Art. 13 EMRK gewährleistete Recht auf eine wirksame Beschwerde; die betreffenden Personen werden nicht angehört und können gegen die Massnahme mangels Kenntnis unmittelbar auch kein Rechtsmittel beziehungsweise Rechtsbehelf ergreifen (vgl. Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 4.3 [nicht publiziert in BGE 149 I 218]). Wie noch zu zeigen sein wird, hat die die Beurteilung, ob ein Regime zur Massenüberwachung konventionskonform ist, gesamthaft unter Berücksichtigung der Anwendung des Regimes zu erfolgen. Zu prüfen wird sein, ob der

innerstaatliche Rechtsrahmen ausreichende Garantien zum Schutz vor Missbrauch enthält. Dabei verlangt der EGMR auch ausreichende verfahrensrechtliche Garantien (vgl. nachfolgend E. 7.3). Vor diesem Hintergrund kommt den in der Konvention und in der Bundesverfassung verankerten Verfahrensgrundrechten für die im vorliegenden Verfahren vorzunehmende Beurteilung ausserhalb des Prüfungsschemas gemäss der Rechtsprechung des EGMR (vgl. hierzu nachfolgend E. 7.3) keine eigenständige Bedeutung zu.

E. 6.5

Als Zwischenergebnis ist festzuhalten, dass die vermutete Bearbeitung von Personendaten der Beschwerdeführenden durch Massnahmen der Funk- und die Kabelaufklärung die Beschwerdeführenden in ihrem Privatleben (Art. 8 Ziff. 1 EMRK; Art. 13 Abs. 1 BV) und jedenfalls die Beschwerdeführenden 4 und 6 in ihrer Medienfreiheit (Art. 10 Ziff. 1 EMRK; Art. 17 BV) beeinträchtigt. Im Folgenden ist zu beurteilen, ob diese Beeinträchtigung gerechtfertigt werden kann (nachfolgend E. 7 ff.). Die beiden Grundrechte stehen dabei nicht in einem Subsidiaritäts- oder Spezialitätsverhältnis zueinander; sie haben jedenfalls in den hier relevanten Teilen getrennte Schutzbereiche und (insoweit) einen unterschiedlichen Schutzzweck (sog. echte Grundrechtskonkurrenz; vgl. hierzu BGE 137 I 167 E. 3.7). Die geltend gemachten Vorbringen sind daher kumulativ zu prüfen. Rechtfertigung der Grundrechtsbeeinträchtigung

E. 7.1

Für die Beurteilung, ob die Beeinträchtigung der Grundrechte gerechtfertigt werden kann, ist im Folgenden zunächst auf das Prüfungsschema einzugehen, das die Grosse Kammer des EGMR zur Beurteilung der Massenüberwachung von Kommunikation entwickelt hat.

E. 7.2

Gemäss Art. 8 Ziff. 2 EMRK darf eine Behörde in das Recht auf Achtung des Privatlebens nur eingreifen, soweit 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. Für die Rechte gemäss Art. 10 EMRK hält die Konvention in Ziff. 2 zunächst fest, dass die Ausübung dieser Freiheiten mit Pflichten und Verantwortung verbunden ist. Sie kann daher 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 (Art. 10 Ziff. 2 EMRK). Gemäss der - im Ergebnis übereinstimmenden - Bestimmung von Art. 36 BV bedürfen Einschränkungen von Grundrechten zunächst einer gesetzlichen Grundlage. Schwerwiegende Einschränkungen müssen im Gesetz selbst vorgesehen sein (Abs. 1). Einschränkungen von Grundrechten müssen zudem durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt (Abs. 2) und verhältnismässig sein (Abs. 3; vgl. BGE 144 I 126 E. 5.1; zum Kerngehalt der Grundrechte gemäss Art. 36 Abs. 4 BV, auf den, wie sich nachfolgend zeigen wird, hier nicht weiter einzugehen ist, vgl. Giovanni Biaggini, Bundesverfassung der Schweizerischen

Eidgenossenschaft, Kommentar, 2. Aufl. 2017, Art. 36 Rz. 24 f. und grundlegend Markus Schefer, Die Kerngehalte von Grundrechten, 2001). Eine schwere Beeinträchtigung eines Grundrechts bedarf einer klaren und ausdrücklichen Regelung in einem formellen Gesetz. Bei einem leichten Eingriff genügt ein Gesetz im materiellen Sinn. Ob ein Eingriff in ein Grundrecht schwer ist, beurteilt sich nach objektiven Kriterien. Nicht entscheidend ist das subjektive Empfinden des Betroffenen (BGE 144 I 126 E. 5.1 mit Hinweisen auf die Rechtsprechung).

E. 7.3.1

Der EGMR hat sich bereits früh mit gezielten Überwachungsmassnahmen insbesondere im Rahmen strafrechtlicher Ermittlungen gegen Einzelpersonen zu befassen gehabt. Dabei wies er stets darauf hin, dass den Staaten bei der Wahl der Mittel zum Erreichen des legitimen Ziels der nationalen Sicherheit ein grosser Ermessensspielraum zukommt (vgl. zit. Urteile Zakharov, § 232, Leander, § 59 und Klass, § 49). Gleichzeitig hielt der EGMR fest (zit. Urteil Zakharov, § 232 [Hervorhebung nur hier]): [...] Cette marge d'appréciation va toutefois de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent. La Cour doit se convaincre de l'existence de garanties adéquates et effectives contre les abus, car un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre. [...] Bei der Beurteilung, ob angemessene und effektive Garantien zum Schutz vor Missbrauch bestehen und die Beeinträchtigung eines Grundrechts mithin gerechtfertigt werden kann, ist nach der Rechtsprechung auf die gesamten Umstände abzustellen, also etwa die Art, den Umfang und die Dauer einer Massnahme, die Gründe und Voraussetzungen für eine Anordnung, die für die Anordnung, Durchführung und Kontrolle zuständigen Behörden und die Art der innerstaatlichen Rechtsbehelfe (zit. Urteil Zakharov, § 232 mit Hinweisen auf die Rechtsprechung; bereits im zit. Urteil Klass, § 50). Der EGMR hat in seiner Rechtsprechung zur gezielten Überwachung der Kommunikation im Rahmen strafrechtlicher Ermittlungen zudem Anforderungen entwickelt, die im Gesetz mindestens festzulegen sind, um Machtbissbrauch zu vermeiden. Konkret verlangt er, dass die (i) Art der Straftaten, die zu einer Überwachungsanordnung führen können, (ii) die Definition der Personengruppen, die einer Überwachung ihrer Kommunikation ausgesetzt sein können, (iii) eine Begrenzung der Dauer der Überwachung, (iv) das bei der Auswertung, Verwendung und Aufbewahrung einzuhaltende Verfahren, (v) die bei der Übermittlung der Daten an andere Stellen zu treffenden Vorkehrungen und (vi) die Umstände, unter denen die Aufzeichnungen gelöscht oder vernichtet werden können oder müssen, gesetzlich geregelt sind (vgl. zit. Urteile Zakharov, § 231 sowie Weber und Saravia, § 95, je mit Hinweisen auf die Rechtsprechung). In seinen Entscheidungen Weber und Saravia sowie Liberty und andere hat der EGMR sodann akzeptiert, dass auch Regime zur Massenüberwachung beziehungsweise strategischen Überwachung nicht per se aus dem Ermessensspielraum der Staaten herausfallen. Darüber hinaus sah er keinen Anlass, die gezielte Überwachung der individuellen Kommunikation und Regime zur allgemeinen Überwachung («les dispositifs de surveillance plus généraux» [zit. Urteil Liberty und andere, § 63]) nach unterschiedlichen Grundsätzen zu beurteilen. Der EGMR verlangte jedoch bezugnehmend auf seine bisherige Rechtsprechung, dass das innerstaatliche Recht wirksame Garantien gegen Missbrauch vorsieht (vgl. zit Urteile Weber und Saravia, §§ 93 ff. sowie § 106 und Liberty und andere, §§ 63 ff.).

E. 7.3.2

In seinen Urteilen Big Brother Watch und andere und Centrum för rättvisa hat die Grosse Kammer des EGMR seine Rechtsprechung zur Massenüberwachung von Kommunikation weiterentwickelt und präzisiert. Dabei hielt der Gerichtshof zunächst an seiner Rechtsprechung fest, wonach die Entscheidung, ein Regime zur Massenüberwachung einzuführen, weiterhin in den Spielraum der einzelnen Staaten fällt (zit. Urteil Big Brother Watch und andere, § 340). Im Weiteren verwies der Gerichtshof auf die technologische Entwicklung und hielt fest, die Art und Weise der Kommunikation habe sich in den letzten zehn Jahren erheblich verändert. Das Leben finde vermehrt online statt und es würden insbesondere erheblich grössere Mengen an Kommunikationsdaten anfallen. Mit diesen sei es möglich, ein persönliches Bild von einer Person zu zeichnen. Der Gerichtshof habe überdies in seinen beiden Entscheiden Weber und Saravia sowie Liberty und andere den Unterschieden zwischen einer gezielten Überwachung und der Massenüberwachung nicht hinreichend Rechnung getragen. So könnten die ersten der beiden Anforderungen an ein System zur gezielten Überwachung (vgl. vorstehend E. 7.3.1) nicht ohne Weiteres auf eine Regelung für die Massenüberwachung angewendet werden. Auch das Erfordernis eines hinreichenden Verdachts, das sich in der Rechtsprechung zur gezielten Überwachung finde, könne im Zusammenhang mit der Massenüberwachung als ein präventives Instrument nicht in gleichem Masse eine Massnahme zum Schutz vor Missbrauch darstellen. Der EGMR wies sodann darauf hin, dass die Massenüberwachung - anders als die gezielte Überwachung - in der Regel auf die internationale Kommunikation ausgerichtet sei. Ihr Zweck sei es beispielsweise, Informationen über Vorgänge im Ausland, mögliche Cyberattacken und Terrorismusbekämpfung zu gewinnen. Gleichwohl könne die Massenüberwachung durch Verwendung sogenannter starker Selektoren auch zur Überwachung konkreter Individuen eingesetzt werden. Die Massenüberwachung habe daher ein beträchtliches Potential, auf eine Weise missbraucht zu werden, die das Recht auf Achtung des Privatlebens beeinträchtige. Während den Mitgliedsstaaten ein weites Ermessen bei der Entscheidung zukommen, welche Art von Überwachungsregime zum Schutz der nationalen Sicherheit notwendig sei, müsse der ihnen gewährte Ermessensspielraum beim Betrieb eines solches enger gefasst sein. Zudem seien hinreichende Massnahmen zum Schutz vor Missbrauch vorzusehen. Vor diesem Hintergrund müssten die bisherigen, für die gezielte Überwachung entwickelten Grundsätze weiterentwickelt werden. Hierbei sei insbesondere dem Umstand Rechnung zu tragen, dass die Massenüberwachung ein schrittweiser Prozess sei und die Intensität des Eingriffs in das Privatleben und die Medienfreiheit im Laufe des Prozesses zunimmt (vgl. vorstehend E. 6.3.2; zit. Urteile Big Brother Watch und andere, §§ 340-347, 348 ff. und Centrum för rättvisa, §§ 254 ff.).

E. 7.3.3

Der EGMR hält mit Blick auf eine Weiterentwicklung der bisherigen Grundsätze fest, das anwendbare Recht müsse mit hinreichender Klarheit die Umstände darlegen, unter denen die Kommunikation überwacht und (mithin) eine Massenüberwachung genehmigt werden dürfe. Zudem sei der Beaufsichtigung und Überprüfung eines Überwachungsregimes verstärktes Gewicht beizumessen; im Zusammenhang mit der Massenüberwachung als ein präventives Instrument bestehe im Vergleich zur gezielten Überwachung, die in der Regel im Rahmen der repressiven strafrechtlichen Verfolgung eingesetzt werden, ein erhöhtes Risiko von Missbrauch. Nach Ansicht des EGMR sind aus diesem Grund durchgehende Garantien («garanties de bout en bout» bzw. «end-to-end-safeguards») zum Schutz vor Missbrauch erforderlich. Das bedeute, dass in jeder Phase der Überwachung (vgl. hierzu

vorstehend E. 6.3.2) eine Beurteilung der Verhältnismässigkeit der gesetzten Massnahmen vorgenommen werden müsse. Der EGMR verlangt vor diesem Hintergrund insbesondere, dass die Massenüberwachung zu Beginn einer unabhängigen Genehmigung und im weiteren Verlauf einer Kontrolle sowie einer unabhängigen nachträglichen Überprüfung («un contrôle indépendant opéré a posteriori») unterworfen wird. Er bezeichnet diese Garantien als «garanties fondamentales», als grundlegende Garantien, die in jedem Fall zu beachten sind, wenn eine Massenüberwachung mit Art. 8 EMRK konform sein soll (zit. Urteil Big Brother Watch und andere, §§ 349 f.; vgl. auch BGE 149 I 218 E. 8.2.2 und 8.11.1; ferner BGE 140 I 353 E. 8.7, wonach Massnahmen der präventiven Überwachung nicht zulässig sind, wenn das anwendbare keine Massnahmen zum Schutz vor Missbrauch wie etwa eine richterliche Genehmigung, die Pflicht zur nachträglichen Mitteilung und Rechtsschutz vorsieht). Zur vorgängigen Genehmigung hält der EGMR fest, dass eine richterliche Genehmigung kein zwingendes Erfordernis darstellt, die Massenüberwachung jedoch in jedem Fall vorgängig von einem von der Exekutive unabhängigen Organ genehmigt werden sollte. Dieses sollte zudem sowohl über den Zweck als auch über die vermutlich zu überwachenden Übertragungsleitungen beziehungsweise Kommunikationswege informiert werden. Damit sei es dem Organ möglich, die Notwendigkeit und Verhältnismässigkeit der Massnahme zu beurteilen. Die Genehmigung sollte zudem zumindest die Arten oder Kategorien der zu verwendenden Selektoren bezeichnen; nach Ansicht des EGMR ist im Prozess der Massenüberwachung die Verwendung von Selektoren einer der wichtigsten Schritte, könnte damit doch die Kommunikation eines bestimmten Individuums anvisiert werden. Zudem sollten verstärkte Garantien vorgesehen werden, wenn sogenannte starke Selektoren zur Anwendung kommen sollen, die mit identifizierbaren Individuen im Zusammenhang stünden. Der EGMR verlangt sodann, dass jede Phase der Massenüberwachung der Beaufsichtigung durch eine unabhängige Behörde zu unterwerfen sei, die über die Befugnis verfüge, den mit der Überwachung verbundenen Eingriff auf das Notwendige zu beschränken. Die Behörde müsse entsprechend in der Lage sein, die Verhältnismässigkeit der gesetzten Handlung zu beurteilen. Der gesamte Prozess der Überwachung sei zudem zu protokollieren beziehungsweise aufzuzeichnen. Nur so sei eine durchgehende Beaufsichtigung überhaupt möglich (vgl. zit. Urteil Big Brother Watch und andere, § 356). Nach der weiterentwickelten Rechtsprechung der Grossen Kammer des EGMR muss zudem jedem, der Verdacht schöpft, dass seine Kommunikation nachrichtendienstlich überwacht werde, ein wirksames Rechtsmittel zur Verfügung stehen, um entweder die Rechtmässigkeit der vermuteten Überwachung oder die Konventionskonformität des Überwachungsregimes in Frage zu stellen. Der EGMR erachtet dabei einen Rechtsbehelf als ausreichend; das Organ, vor dem der Rechtsbehelf erhoben werden kann, muss nicht zwingend ein richterliches, aber doch ein von der Exekutive unabhängiges Organ sein, das die Fairness des Verfahrens sicherstellt und soweit möglich im Rahmen eines kontradiktorischen Verfahrens entscheidet. Die Entscheide eines solchen Organs müssen sodann begründet und rechtlich verbindlich sein (vgl. zit. Urteil Big Brother Watch und andere, §§ 357-359). Für die Beurteilung, ob ein Regime der Massenüberwachung konform ist mit der EMRK, hält der EGMR schliesslich fest (zit. Urteil Big Brother Watch und andere, § 360 [Hervorhebungen nur hier]: Au vu de ce qui précède, la Cour devra, pour se prononcer sur la conformité à la Convention d'un régime d'interception en masse, en apprécier globalement le fonctionnement. À cet effet, elle recherchera principalement si le cadre juridique interne contient des garanties suffisantes contre les abus et si le processus est assujetti à des «

garanties de bout en bout » (...). Ce faisant, elle tiendra compte de la mise en oeuvre effective du système d'interception, notamment des freins et contrepoids à l'exercice du pouvoir et de l'existence ou de l'absence de signes d'abus réels (...). Konkret prüfte der EGMR im Rahmen seiner beiden Entscheidungen Big Brother Watch und andere und Centrum för rättvisa, ob das innerstaatliche Recht die folgenden Aspekte eindeutig festlegte (zit. Urteile Big Brother Watch und andere, § 361 und Centrum för rättvisa, § 284): 1) die Gründe, aus denen eine Massenüberwachung genehmigt werden darf; («Les motifs pour lesquels l'interception en masse peut être autorisée») 2) die Umstände, unter denen die Kommunikation eines Individuums überwacht werden darf; («Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées») 3) das für die Erteilung der Genehmigung einzuhaltende Verfahren; («La procédure d'octroi d'une autorisation») 4) die für die Auswahl, Auswertung und Verwendung des abgefangenen Materials einzuhaltenden Verfahren; («Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés») 5) die zu treffenden Vorkehrungen, wenn Material an andere Parteien übermittelt wird; («Les précautions à prendre pour la communication de ces éléments à d'autres parties») 6) die Grenzen für die Dauer der Überwachung und Aufbewahrung von abgefangenem Material und die Umstände, unter denen solches Material gelöscht und zerstört werden muss; («Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits») 7) die Verfahren und Modalitäten für die Kontrolle durch eine unabhängige Behörde im Hinblick auf die Einhaltung der Garantien und deren Befugnisse im Falle der Nichteinhaltung; («Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement») 8) das Verfahren für eine unabhängige nachträgliche Überprüfung der Einhaltung der Garantien und die Befugnisse des zuständigen Organs für den Fall der Nichteinhaltung. («Les procédures de contrôle indépendant a posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement») Der EGMR prüfte anhand dieser acht Punkte, ob das innerstaatliche (Verfahrens-)Recht zugänglich war und es hinreichende und wirksame Garantien zum Schutz vor Missbrauch («garanties et des garde-fous effectifs et suffisants» bzw. «adequate and effective safeguards and guarantees») vorsah, um die Anforderung der Vorhersehbarkeit und der Verhältnismässigkeit zu erfüllen (zit. Urteil Big Brother Watch und andere, § 365). Dabei berücksichtigte er auch, ob es in der Praxis Hinweise auf Missbrauch der Überwachungsbefugnisse gibt (zit. Urteile Centrum för rättvisa, § 274 und Ekimdzhiev und andere, § 293). Der EGMR ging zudem davon aus, dass die Erlangung von Kommunikationsranddaten durch Massenüberwachung die berührten Grundrechte in vergleichbarem Mass beeinträchtigt wie die Erlangung von Inhalten der Kommunikation. Er prüfte aus diesem Grund das Abfangen, Speichern und Durchsuchen von Randdaten ebenfalls nach den vorstehend dargestellten Grundsätzen (vgl. zit. Urteil Big Brother Watch und andere, § 363; vgl. zum Ganzen auch Christian Maierhöfer, in: Frowein/Peukert, EMRK-Kommentar, 4. Aufl. 2024, Art. 8 Rz. 67 mit Hinweisen). Das deutsche Bundesverfassungsgericht beurteilt die Massenüberwachung - im deutschen Recht als strategische Telekommunikationsüberwachung bezeichnet - nach einem vergleichbaren Ansatz (vgl. die Systematik im zitierten Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, insbes. Bst. E Ziffn. I. - V.). Im Rahmen der nachfolgenden materiellen Beurteilung, ob der Eingriff in die Grund- und Konventionsrechte der Beschwerdeführenden gerechtfertigt werden kann, ist daher

vergleichend auch die Rechtsprechung des deutschen Bundesverfassungsgerichts zur Ausland-Ausland- und zur Inland-Ausland-Fernmeldeaufklärung zu berücksichtigen (vgl. in diesem Sinne bereits der Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 6.2.3 und E. 8.2).

E. 7.4

Der dargestellte, von der Grossen Kammer des EGMR betreffend die Massenüberwachung entwickelte Beurteilungsrahmen ist auch im vorliegenden Verfahren zur Beurteilung der Funk- und Kabelaufklärung anzuwenden (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 11). Es ist mithin zu prüfen, ob das für die Funk- und Kabelaufklärung anwendbare Recht die geforderten Aspekte regelt und insgesamt - unter Berücksichtigung der tatsächlichen Funktionsweise - hinreichenden und wirksamen Schutz vor Missbrauch bietet. Der EGMR geht in seiner Rechtsprechung und mit Blick auf die an ein Regime der Massenüberwachung gestellten Anforderungen davon aus, dass die Frage, ob eine Massnahme gesetzlich vorgesehen ist, in einem engen Zusammenhang steht mit der Frage, ob diese in einer demokratischen Gesellschaft notwendig ist. So müsse das anwendbare Recht nicht nur zugänglich und in seiner Anwendung vorhersehbar sein. Es sei vielmehr, wie bereits ausgeführt, auch erforderlich, dass das anwendbare Recht wirksamen Schutz vor Missbrauch biete und entsprechende Garantien vorsehe. Der Gerichtshof erachtet es daher als angezeigt, die Anforderungen «gesetzlich vorgesehen» und «in einer demokratischen Gesellschaft notwendig» gemeinsam und nicht in getrennten Prüfungsschritten zu beurteilen (vgl. zit. Urteile Big Brother Watch und andere, § 334 und Centrum för rättvisa, § 248, je mit Hinweisen auf die Rechtsprechung; ferner auch BGE 148 I 233 E. 4.2 in fine, wonach die gesetzliche Grundlage einen angemessenen Rechtsschutz gegen Willkür bieten muss). In diesem Sinne ist auch hier vorzugehen. Die Voraussetzungen zur Rechtfertigung der Beeinträchtigung der Grundrechte (Art. 8 Ziff. 2 und Art. 10 Ziff. 2 EMRK sowie Art. 36 BV) sind im Rahmen der vorerwähnten acht Prüfpunkte gemeinsam zu prüfen. Die Prüfung ist zudem gleichzeitig in Bezug sowohl auf die Überwachung des Inhalts der elektronischen Kommunikation als auch der damit verbundenen Randdaten durchzuführen; für die Überwachung des Inhalts und der Randdaten der Kommunikation gelten (im Wesentlichen) dieselben Rechtsvorschriften (vgl. zit. Urteil Centrum för rättvisa, § 283). Und schliesslich ist die Prüfung - insbesondere zur Vermeidung von Wiederholungen - auch gleichzeitig für die beiden beeinträchtigten Grund- und Konventionsrechte vorzunehmen. Die Rechtsbegehren der Beschwerdeführenden beziehen sich auf die Funk- und Kabelaufklärung; es wird verlangt, die Funk- und Kabelaufklärung einzustellen (vgl. vorstehend Sachverhalt Bst. A.a). Gemäss der Beschwerdebegründung und den weiteren Rechtsschriften sehen die Beschwerdeführenden ihre durch die Bundesverfassung und die EMRK garantierten Rechts jedoch in erster Linie durch die Kabelaufklärung verletzt. Die Beurteilung des Regimes der Kabelaufklärung steht daher im Zentrum der nachstehenden Beurteilung. Entsprechend den Rechtsbegehren der Beschwerdeführenden ist dabei gleichzeitig auch auf die Funkaufklärung einzugehen. Hierzu verpflichtet auch der Rückweisungsentscheid des Bundesgerichts.

E. 7.5

Das anwendbare Recht muss für die betroffenen Personen zugänglich und in seinen Auswirkungen vorhersehbar sein. Im Zusammenhang mit präventiven Überwachungsmassnahmen kann die geforderte Vorhersehbarkeit jedoch nicht bedeuten, dass der Einzelne in der Lage ist, vorherzusehen, wann die Behörde wahrscheinlich zu

solchen Massnahmen greifen wird, damit er sein Verhalten entsprechend danach richten kann und die Überwachung damit allenfalls vereitelt oder umgangen würde. Geheime Überwachungsmassnahmen wie die Funk- und Kabelaufklärung gelangen den Betroffenen jedoch grundsätzlich nicht zur Kenntnis; auch aufgrund ihres Charakters als Instrument der anlasslosen Massenüberwachung erfolgt anders als bei genehmigungspflichtigen Beschaffungsmassnahmen (Art. 33 NDG) keine Benachrichtigung. Ein ordentliches Rechtsmittel, das eine Beurteilung ex ante erlauben würde, besteht entsprechend nicht (vgl. zur nachträglichen Überprüfung nachfolgend E. 22-24). Dies hat zur Folge, dass der Gehalt der gesetzlichen Regelung nur eingeschränkt - im Rahmen des Genehmigungsverfahrens - im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden kann. Das anwendbare Recht muss daher auch im Zusammenhang mit der Überwachung der Kommunikation hinreichend bestimmt sein, so dass es den Bürgern einen Hinweis darauf zu geben vermag, unter welchen Umständen und unter welchen Bedingungen Behörden im Allgemeinen befugt sind, auf die Massnahmen der Funk- und Kabelaufklärung zurückzugreifen (zit. Urteile Big Brother Watch und andere, §§ 332 f. und Centrum för rättvisa, §§ 246 f.; vgl. zudem den zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Ziff. 154).

E. 7.6.1

Im Folgenden ist anhand der dargelegten Prüfpunkte zu beurteilen, ob die mit der Funk- und Kabelaufklärung einhergehende Beeinträchtigung des Privatlebens und der Medienfreiheit gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist (Art. 8 Ziff. 2 und Art. 10 Ziff. 2 EMRK; vgl. auch Art. 36 BV). Hierfür ist zunächst auf die Schwere der Beeinträchtigung einzugehen (nachfolgend E. 7.6.2); die Schwere der Beeinträchtigung ist bei der Beurteilung der Notwendigkeit beziehungsweise der Verhältnismässigkeit von Bedeutung. Die Vorinstanz, der Beigeladene und weitere Behörden haben zudem die von ihnen beigebrachten Unterlagen teilweise als vertraulich beziehungsweise als nur für das Bundesverwaltungsgericht bestimmt bezeichnet. Die Vorinstanz und der Beigeladene verweisen zur Begründung im Wesentlichen auf den Schutz technischer Quellen. Es ist daher ebenfalls vorab zu prüfen, ob und in welchem Rahmen der Schutz technischer Quellen die Vertraulichkeit beziehungsweise Geheimhaltung der beigebrachten Unterlagen rechtfertigt (nachfolgend E. 7.6.3).

E. 7.6.2

Die Grosse Kammer des EGMR beschreibt Massenüberwachungen wie die Funk- und Kabelaufklärung in verschiedenen Phasen beziehungsweise als einen schrittweisen Prozess, bei dem die Intensität des Eingriffs in die Ausübung des Rechts auf Achtung des Privatlebens und der Freiheit der Meinungsäusserung im Laufe des Prozesses zunimmt (vgl. bereits vorstehend E. 6.3.2). Das anfängliche Erfassen und unmittelbare Aussortieren von Teilen der Kommunikation stellt nach Ansicht des EGMR keine besonders schwerwiegende Beeinträchtigung der berührten Grundrechte dar. Das Ausmass der Beeinträchtigung nehme zu, je weiter der Prozess voranschreite. Die Notwendigkeit von Garantien zum Schutz vor Missbrauch sei dabei höher, wenn Personendaten automatisiert ausgewertet würden. Am Ende des Prozesses, wenn Informationen über eine bestimmte Person von einem Analytiker untersucht und alsdann verwendet würden, sei der Bedarf an Massnahmen zum Schutz vor Missbrauch am grössten (zit. Urteil Big Brother Watch und andere, §§ 330 und 450). Auch für die Funk- und Kabelaufklärung ist davon auszugehen, dass die Schwere der Beeinträchtigung im Verlaufe des Auswertungsprozesses zunimmt, wobei die mit der Funk-

und Kabelaufklärung verbundenen Beeinträchtigung der berührten Grundrechte schliesslich besonders schwer wiegt. Ausgangspunkt ist insoweit, dass jede heimliche Massenüberwachung der Telekommunikation grundsätzlich einen schweren Eingriff in das Recht auf Achtung des Privatlebens darstellt; Kommunikation hat oftmals privaten und unter Umständen sogar höchstpersönlichen Charakter. Erschwerend fällt sodann insbesondere die Anlasslosigkeit in Betracht (vgl. in diesem Sinne auch BGE 151 I 137 E. 3.3.2). Die Funk- und Kabelaufklärung werden im Wesentlichen final durch ihren Zweck und damit nur in eingeschränktem Masse gesetzlich angeleitet. Sie verfügen zudem über eine ausserordentliche Reichweite, was die Schwere der Beeinträchtigung zusätzlich erhöht. Schliesslich wird im Rahmen der Funk- und Kabelaufklärung auch die Kommunikation von Personen im Inland erfasst und bearbeitet; die Verwendung im Rahmen der Kabelaufklärung ist dann nicht zulässig, wenn sich sowohl der Sender als auch der Empfänger in der Schweiz befinden (Art. 39 Abs. 2 NDG). Die Schwere der Beeinträchtigung wird schliesslich dadurch gemildert, dass die Funk- und Kabelaufklärung im Vergleich zur Überwachung der individuellen Kommunikation weniger zielgenau sind und, da sie der Beschaffung von Informationen über sicherheitspolitisch relevante Vorgänge im Ausland dienen, grundsätzlich keine unmittelbaren Konsequenzen für den Einzelnen hat (vgl. hierzu auch den zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Ziffn. 157-160; zu den Kriterien, die einer Beurteilung der Schwere der Beeinträchtigung zu Grunde zu legen sind, auch Hecker, a.a.O., III § 2 Rz. 31). Insgesamt ist daher hier für die weitere Prüfung von einer schweren Beeinträchtigung des Anspruchs auf Achtung des Privatlebens und der Medienfreiheit auszugehen.

E. 7.6.3

Die Vorinstanz hat dem Bundesverwaltungsgericht mehrere Vernehmlassungen und Stellungnahmen eingereicht. Diese sind teilweise in einer parteiöffentlichen und in einer nur für das Gericht bestimmten Version mit weitergehenden Ausführungen eingereicht worden, wobei die Vorinstanz zur Begründung auf die Vertraulichkeit der betreffenden Ausführungen verweist. Zudem haben die Vorinstanz, der Beigeladene und die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI dem Bundesverwaltungsgericht mehrere als vertraulich beziehungsweise geheim bezeichnete Unterlagen eingereicht. Die Beschwerdeführenden haben wiederholt um (weitergehende) Einsicht in die Vernehmlassungen beziehungsweise Stellungnahmen und in die von der Vorinstanz, dem Beigeladenen sowie der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI eingereichten Unterlagen ersucht. Die Beschwerdeführenden haben gemäss Ar. 29 Abs. 2 BV Anspruch auf rechtliches Gehör. Das Verfahrensgrundrecht umfasst als Teilgehalt den Anspruch auf Akteneinsicht, der für das Beschwerdeverfahren in den Art. 26-28 VwVG konkretisiert wird. Der Anspruch auf Akteneinsicht bezieht sich auf sämtliche verfahrensbezogenen Akten, die geeignet sind, Grundlage des Entscheids zu bilden (vgl. Art. 26 Abs. 1 VwVG). Der Anspruch besteht unabhängig davon, ob die Ausübung des Akteneinsichtsrechts den Entscheid in der Sache zu beeinflussen zu vermag. Die Einsicht in Akten, die für ein bestimmtes Verfahren erstellt oder beigezogen wurden, kann demnach grundsätzlich nicht mit der Begründung verweigert werden, die fraglichen Akten seien für den Verfahrensausgang ohne Bedeutung; es ist Sache der Parteien, die Relevanz der Akten zu beurteilen (BGE 144 II 427 E. 3.1.1; Urteil des BGer 1C_347/2024 vom 14. Oktober 2024 E. 2.2 mit Hinweis). Der Anspruch auf Akteneinsicht gilt nicht absolut. Er kann beschränkt oder verweigert werden, wenn und soweit ein überwiegendes öffentliches Interesse oder berechtigte Geheimhaltungsinteressen Privater entgegenstehen

(vgl. Art. 27 Abs. 1 VwVG). Dabei ist ein materieller Geheimnisbegriff massgebend, weshalb allein die Klassifizierung von Unterlagen gemäss der Informationsschutzverordnung (ISchV, SR 510.411) nicht entscheidend ist. Vielmehr sind die berührten Interessen sorgfältig gegeneinander abzuwägen, wobei die Klassifizierung eines Dokuments ein Indiz für das Vorliegen von Verweigerungsgründen ist. Die Verweigerung der Einsichtnahme darf sich gemäss Art. 27 Abs. 2 VwVG nur auf die Aktenstücke erstrecken, für die Geheimhaltungsgründe bestehen (vgl. BGE 147 I 463 E. 3.3.3 und Urteil des BGer 2C_602/2018 vom 16. September 2019 E. 3.3.1, je mit Hinweisen). Wird einer Partei die Einsichtnahme in ein Aktenstück gemäss Art. 27 VwVG verweigert, so darf auf dieses zum Nachteil der Partei nur abgestellt werden, wenn ihr die Behörde von seinem für die Sache wesentlichen Inhalt Kenntnis und ihr ausserdem Gelegenheit gegeben hat, sich zu äussern und Gegenbeweismittel zu bezeichnen (Art. 28 VwVG). Der Grundsatz gemäss Art. 28 VwVG ergibt sich bereits aus dem Verfahrensgrundrecht gemäss Art. 29 Abs. 2 BV (Urteil des BGer 1C_415/2019 vom 27. März 2020 E. 2.3.1 mit Hinweis unter anderem auf BGE 115 Ia 293 E. 5c). Das Nachrichtendienstgesetz regelt in Art. 35 den Quellenschutz. Demnach hat die Vorinstanz den Quellenschutz sicherzustellen (Art. 35 Abs. 1 NDG). Das Ziel ist der Fortbestand der Quelle zur Informationsgewinnung, wobei das Gesetz zwischen menschlichen und technischen Quellen unterscheidet (vgl. Botschaft NDG, BBl 2014 2105, 2173 f.). Der Schutz einer Quelle ist sodann grundsätzlich gleichbedeutend mit der Geheimhaltung entsprechender Informationen. Bei technischen Quellen umfasst der Schutz in sachlicher Hinsicht geheimhaltungsbedürftige Angaben über Infrastruktur, Leistungsfähigkeit, operative Methoden und Verfahren der Informationsbeschaffung (Art. 35 Abs. 3 Bst. c NDG). Gemäss Art. 18 Abs. 5 NDV sind bei technischen Quellen (somit) alle Angaben zu schützen und mithin geheim zu halten, ausser wenn die Bekanntgabe die Auftragserfüllung der Vorinstanz weder direkt noch indirekt gefährdet. Entsprechend ist in den Materialien zum Nachrichtendienstgesetz als Grundsatz in allgemeiner Weise festgehalten, dass die Wahrung des Quellenschutzes für die Vorinstanz von grösster Bedeutung ist. Quellen sollen nur ausnahmsweise preisgegeben werden, wenn das öffentliche Interesse an der Preisgabe weit überwiegt (Botschaft NDG, BBl 2014 2105, 2173). Die Vorinstanz hat dem Bundesverwaltungsgericht auf Verlangen hin die Leistungsausweise COMINT für die Jahre 2019 - 2024, den Bericht mit einer Bilanz zur Kabelaufklärung während der Aufbauphase und eine Liste der Kategorien von Suchbegriffen in der Kabelaufklärung (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 4) zu den Akten gegeben (vgl. vorstehende Sachverhalt Bst. K.h, Q.c, S.e und Y.c). Die Leistungsausweise, der Bericht und die Liste der Kategorien von Suchbegriffen sind als geheim klassifiziert. Die Leistungsausweise geben Auskunft über die Gesamtproduktion des Beigeladenen im Bereich der Funk- und Kabelaufklärung und enthalten hierzu konkrete Angaben zum Aufbau und zur Entwicklung der Kabelaufklärung, zu Aufträgen und Resultaten (einschliesslich Darstellung von Fällen mit einem Schweiz-Bezug und damit verbunden der Praxis zur [Ent-]Anonymisierung), aufgeteilt nach verschiedenen Aufklärungsgebieten, zur Zusammenarbeit mit Partnerdiensten, zu technischen Möglichkeiten, Grenzen und Entwicklungen sowie zum Zusammenwirken zwischen den verschiedenen zur Verfügung stehenden Sensoren. Vergleichbare Informationen ergeben sich auch aus dem Bericht mit einer Bilanz zur Kabelaufklärung. Dieser enthält zusätzlich eine umfangreiche Bewertung des Instruments Kabelaufklärung durch die Vorinstanz, einschliesslich Angaben zur technischen Infrastruktur des Beigeladenen und zu den verpflichteten Betreiberinnen von

leitungsgebundenen Netzen beziehungsweise Anbieterinnen von Fernmeldedienstleistungen, sowie zu Resultaten aus der Kabelaufklärung und zur Genehmigungspraxis des Bundesverwaltungsgerichts (Abteilung I, Fachgebiet NDG). Der Bericht mit einer Bilanz zur Kabelaufklärung gibt sodann Einblick in die weitere Entwicklung und künftige Ausrichtung der Kabelaufklärung, während die Liste mit den Suchbegriffen für die Kabelaufklärung Rückschlüsse auf die (laufenden) Aufträge für die Kabelaufklärung zulässt. Die in den Leistungsausweisen, im Bericht und in der Liste enthaltenen Informationen stehen in einem direkten Zusammenhang zur Wahrung der inneren und äusseren Sicherheit der Schweiz. Es kann daher weder Akteneinsicht gewährt, noch kann der wesentliche Inhalt bekannt gegeben werden. Unter diesen Umständen dürfte das Bundesverwaltungsgericht bei seiner Entscheidung grundsätzlich nicht auf die Leistungsausweise, den Bericht und die Liste abstellen, ansonsten das Verfahrensgrundrecht gemäss Art. 29 Abs. 2 BV verletzt würde. Gemäss dem Rückweisungsentscheid des Bundesgerichts 1C_377/2019 hat das Bundesverwaltungsgericht jedoch zu prüfen, ob die vermutete Bearbeitung von Daten der Beschwerdeführenden im Rahmen der Funk- und Kabelaufklärung deren Grundrechte verletzt. Hierbei sind auch allfällige interne Richtlinien und Weisungen, die effektive Vollzugspraxis und die tatsächliche Kontrollpraxis der Aufsichtsbehörden zu berücksichtigen. Der Anspruch auf diese Prüfung ergibt sich aus Art. 13 EMRK - und liegt damit im Interesse Beschwerdeführenden (vgl. Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020, insbes. E. 7-9; vgl. in diesem Sinne auch Urteil des BGer 1C_518/2013 vom 1. Oktober 2014 E. 2 [nicht veröffentlicht in BGE 140 I 381]). Unter diesen Umständen ist dem Interesse an einer effektiven Überprüfung der vermuteten Bearbeitung von Daten der Beschwerdeführenden (Art. 13 EMRK) das höhere Gewicht beizugeben als dem verfassungsmässigen Anspruch auf rechtliches Gehör (Art. 29 Abs. 2 BV). Die Gesuche der Beschwerdeführenden um Einsicht in die Leistungsausweise COMINT, in den Bericht mit einer Bilanz zur Kabelaufklärung und in die Liste der Kategorien von Suchbegriffen in der Kabelaufklärung sind daher abzuweisen. Die Leistungsausweise, der Bericht und die Liste sind zudem als Grundlage für den vorliegenden Entscheid in den Akten zu belassen, ohne dass den Beschwerdeführenden deren wesentlicher Inhalt bekannt gegeben wird. Die Vorinstanz, der Beigeladene und die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI haben dem Bundesverwaltungsgericht zudem weitere vertrauliche Angaben gemacht beziehungsweise als vertraulich gekennzeichnete Unterlagen zu den Akten gegeben. Diese Angaben und Unterlagen sind grundsätzlich geeignet, Grundlage des Entscheids zu bilden. Die Gesuche der Beschwerdeführenden um Akteneinsicht wären daher gutzuheissen, soweit nicht überwiegende öffentliche Interessen entgegenstehen. Auch die vertraulichen Angaben und die als vertraulich bezeichneten Unterlagen enthalten jedoch Angaben über das Vorgehen beziehungsweise das Verfahren der Informationsbeschaffung oder lassen zumindest Rückschlüsse darauf zu. Grundsätzlich besteht somit ein öffentliches Interesse von erheblichem Gewicht, das die Geheimhaltung der Angaben und Unterlagen erfordert. Zudem ist es (für das Bundesverwaltungsgericht) nicht möglich, abschliessend zu beurteilen, welche Rückschlüsse aus den betreffenden Angaben und Unterlagen in Bezug auf die Fernmeldeüberwachung tatsächlich gezogen werden könnten. Das Bundesverwaltungsgericht hat aus diesen Gründen das Gesuch um Akteneinsicht der Beschwerdeführenden in Bezug auf bestimmte Angaben und Unterlagen mit Zwischenverfügungen vom 2. und 9. September 2025 abgewiesen. Gleichzeitig hat es den Beschwerdeführenden, soweit für das vorliegende Urteil erheblich, den wesentlichen

Inhalt der Angaben und Unterlagen bekannt gegeben (vgl. vorstehend Sachverhalt Bst. Y.a und Y.b). Soweit die Vorinstanz und der Beigeladene weitergehende vertrauliche Angaben gemacht und als vertraulich bezeichnete Unterlagen zu den Akten gegeben haben, ist das das Gesuch der Beschwerdeführenden um Akteneinsicht ebenfalls abzuweisen. Damit wäre den Beschwerdeführenden grundsätzlich der wesentliche Inhalt bekannt zu geben und ihnen das rechtliche Gehör zu gewähren. Der Bestimmung von Art. 35 Abs. 1 NDG liegt jedoch die generell-abstrakte Wertung zu Grunde, Angaben zu technischen Quellen nur ausnahmsweise und bei weit überwiegenden öffentlichen Interessen bekannt zu geben. Es ist daher hier vom Grundsatz abzuweichen, dass sich der Umfang des Rechts auf Akteneinsicht nach der Eignung der Akten bestimmt, Grundlage des Entscheids zu bilden. Vielmehr ist den Beschwerdeführenden der wesentliche Inhalt nur jener Akten bekannt zu geben, die für den Entscheid erheblich sind. Entsprechendes hat das Bundesverwaltungsgericht mit Zwischenverfügungen vom 2. und 9. September 2025 bereits verfügt. In Bezug auf die weiteren vertraulichen Angaben und Unterlagen, die für den vorliegenden Entscheid nicht erheblich sind, ist das Gesuch um Akteneinsicht abzuweisen und darauf zu verzichten, den Beschwerdeführenden den wesentlichen Inhalt bekannt zu geben. Damit geht eine Beschränkung des Anspruchs auf rechtliches Gehör einher, umso mehr, als nicht die Parteien selbst - nach erfolgter Einsicht in die Akten - die Erheblichkeit der Angaben und Unterlagen beurteilen können, sondern diese Beurteilung vom Bundesverwaltungsgericht vorgenommen wird. Für diese Beeinträchtigung besteht jedoch mit Art. 35 NDG eine gesetzliche Grundlage und sie erweist sich Blick auf das berührte öffentliche Interesse der inneren und äusseren Sicherheit hier insgesamt auch als verhältnismässig. Prüfpunkt 1 Gründe, aus denen eine Massenüberwachung genehmigt werden darf

E. 8.1

Nach der Rechtsprechung des EGMR ist sind die Gründe, aus denen eine Massenüberwachung angeordnet werden darf, möglichst eng zu fassen und klar zu bestimmen; je weiter und unbestimmter die Gründe sind, umso grösser ist die Gefahr des Missbrauchs. Ein Regime, das erlaubt, eine Massenüberwachung aus relativ weiten Gründen anzuordnen, kann jedoch gleichwohl mit Art. 8 EMRK in Einklang stehen. Hierzu ist erforderlich, dass das anwendbare Recht insgesamt hinreichenden und insbesondere wirksamen Schutz vor Missbrauch bietet. Der Mangel einer (zu) weit gefassten Regelung würde damit ausgeglichen (vgl. zit. Urteil Big Brother Watch und andere, § 370; zudem den zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Ziff. 164). Das Bundesgericht stellt in seiner Rechtsprechung vergleichbare Anforderungen an die Regelungsdichte. Demnach verlangt das Legalitätsprinzip (Art. 36 Abs. 1 BV) im Interesse der Rechtssicherheit und der rechtgleichen Rechtsanwendung eine hinreichende und angemessene Bestimmtheit der anzuwendenden Rechtssätze. Diese müssen so präzise formuliert sein, dass die Rechtsunterworfenen ihr Verhalten danach ausrichten und die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Gewissheit erkennen können. Beim Sammeln und Speichern von Daten etwa muss die gesetzliche Grundlage so gefasst sein, dass es jeder Person möglich ist - erforderlichenfalls bei einer entsprechenden Rechtsberatung -, die möglichen Auswirkungen ihres Verhaltens auf ihr Recht auf informationelle Selbstbestimmung abzuschätzen (BGE 148 I 233 E. 4.2 mit Hinweisen auf die Rechtsprechung des Bundesgerichts und des EGMR). In anderen Rechtsgebieten wie etwa dem Polizeirecht, in denen das Bestimmtheitserfordernis aufgrund des Regelungsbereichs an seine Grenzen stösst, kann die Unbestimmtheit von Normen

durch verfahrensrechtliche Garantien kompensiert werden. In solchen Fällen kommt zudem dem Grundsatz der Verhältnismässigkeit in besondere Bedeutung zu; wo die Unbestimmtheit von Rechtssätzen zu einem Verlust an Rechtssicherheit führt, muss die Verhältnismässigkeit umso strenger geprüft werden. Insgesamt hängt der Grad der erforderlichen Bestimmtheit insbesondere von der Vielfalt der zu ordnenden Sachverhalte, von der Komplexität und von der erst bei der Konkretisierung im Einzelfall möglichen und sachgerechten Entscheidung ab (BGE 144 I 126 E. 6.1 mit Hinweisen; vgl. auch BGE 151 I 137 E. 4.5.1 und BGE 140 I 381 E. 4.4, die abstrakte Normenkontrolle betreffend und je mit Hinweisen auf die Rechtsprechung).

E. 8.2

Im Urteil Big Brother Watch und andere hatte der EGMR unter anderem zu beurteilen, ob das Vereinigte Königreicht durch den damaligen Regulation of Investigatory Powers Act 2000 (nachfolgend: RIPA), der Massnahmen zur Überwachung der elektronischen Kommunikation zulässt, das Privatleben und die Medienfreiheit beeinträchtigt und ob die Beeinträchtigung gerechtfertigt werden kann. Gemäss dem RIPA konnten Überwachungen im Interesse der nationalen Sicherheit, zur Verhütung oder Aufdeckung schwerer Straftaten oder zur Wahrung des wirtschaftlichen Wohls des Vereinigten Königreichs angeordnet werden. Nach Ansicht des EGMR fasste das Vereinigte Königreich damit die Gründe, aus denen eine Massenüberwachung angeordnet werden darf, relativ weit. Der EGMR überprüfte in der Folge, ob die Regelung gemäss dem RIPA insgesamt den Anforderungen von Art. 8 und Art. 10 EMRK genügte - und verneinte dies (zit. Urteil Big Brother Watch und andere, §§ 371, 424 ff. und 456 ff.). Demgegenüber erachtete der EGMR in seiner Entscheidung Centrum för rättvisa den Bereich, in dem die Massenüberwachung nach Massgabe des damaligen schwedischen Gesetzes eingesetzt wurde, als hinreichend klar umrissen, insbesondere, da die angefochtene Regelung darauf abzielte, unbekannte ausländische Bedrohungen aufzudecken, deren Art sich im Verlaufe der Zeit ändern und weiterentwickeln könnten. So durfte eine Massnahme etwa angeordnet werden zur Überwachung einer externen militärischen Bedrohung, in Bezug auf internationalen Terrorismus und andere schwere grenzüberschreitende Verbrechen, die Entwicklung und Verbreitung von Massenvernichtungswaffen oder ausländische Konflikte mit Auswirkungen auf die internationale Sicherheit (zit. Urteil Centrum för rättvisa, §§ 284 f.; vgl., zu den beiden Urteilen auch Maierhöfer, a.a.O., Art. 8 Rz. 47 mit Hinweisen). Im Folgenden ist zu prüfen, ob das anwendbare Recht die Gründe, aus denen eine Kabelaufklärung genehmigt beziehungsweise eine Funkaufklärung eingesetzt werden darf, hinreichend bestimmt festlegt und ob die Gründe die Beeinträchtigung der durch Bundesverfassung und EMRK garantierte Rechte zu rechtfertigen vermögen, es sich mithin um zulässige Gründe handelt.

E. 9.1

Die Vorinstanz kann den Beigeladenen im Rahmen einer Kabelaufklärung damit beauftragen, zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland gemäss Art. 6 Abs. 1 Bst. b NDG sowie zur Wahrung weiterer wichtiger Landesinteressen gemäss Art. 3 NDG grenzüberschreitende Signale aus leitungsgebundenen Netzen zu erfassen (Art. 39 Abs. 1 NDG). Als weitere wichtige Landesinteressen nennt Art. 3 NDG den Schutz der verfassungsrechtlichen Grundordnung der Schweiz (Bst. a), die Unterstützung der schweizerischen Aussenpolitik (Bst. b) und den Schutz des Werk-, Wirtschafts- und Finanzplatzes Schweiz (Bst. c). Gemäss den

Materialien bezieht sich der Begriff «sicherheitspolitisch bedeutsame Vorgänge im Ausland» auf Ereignisse und Entwicklungen im Ausland, die geeignet sind, die Selbstbestimmung der Schweiz und ihre demokratische und rechtsstaatliche Ordnung zu gefährden, der Schweiz schweren sicherheitspolitischen oder anderweitigen Schaden zuzufügen oder die Handlungsfähigkeit ihrer Behörden zu beeinträchtigen. In diesem Zusammenhang erbringt die Vorinstanz hauptsächlich Leistungen für das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) in Form von analytischen Berichten und Übermittlung von Einzelinformationen (Botschaft NDG, BBl 2014 2105, 2143). Der Bund kann sodann - und tut es auch - einen Dienst für die Erfassung elektromagnetischer Ausstrahlungen von Telekommunikationssystemen, die sich im Ausland befinden, betreiben (sog. Funkaufklärung; Art. 38 Abs. 1 NDG). 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 im Sinne von Art. 3 NDG. Weitere Einzelheiten regelt der Bundesrat auf Verordnungsstufe (Art. 38 Abs. 3 NDG).

E. 9.2

Der Zweck der Kabelaufklärung wird auf Verordnungsstufe in Art. 25 NDV konkretisiert: Art. 25Zweck der Kabelaufklärung Der NDB kann durch Kabelaufklärung sicherheitspolitisch bedeutsame Informationen insbesondere in den folgenden Bereichen zu den nachstehenden Zwecken beschaffen: a. im Bereich Terrorismus: zur Erkennung von Aktivitäten, Verbindungen und Strukturen von terroristischen Gruppierungen und Netzwerken sowie zur Erkennung von Aktivitäten und Verbindungen von Einzeltäterinnen und Einzeltätern; b. im Bereich Proliferation: zur Aufklärung von 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), zur Aufklärung von illegalem Handel mit radioaktiven Substanzen, Kriegsmaterial und anderen Rüstungsgütern, zur Aufklärung von Programmen für Massenvernichtungswaffen, einschliesslich ihrer Trägersysteme, sowie zur Aufklärung von Beschaffungsstrukturen und Beschaffungsversuchen; c. im Bereich Spionageabwehr: zur Erkennung von Aktivitäten und Strukturen staatlicher und nichtstaatlicher ausländischer Akteure; d. im Bereich ausländische, gegen die Schweiz gerichtete Handlungen und Motive sowie ausländische Handlungen oder Konflikte mit Auswirkungen auf die Schweiz: zur Beurteilung von Sicherheitslage, Regimestabilität, militärischem Potenzial und Rüstungsentwicklung, strategischen Einflussfaktoren und möglichen Entwicklungen; e. in den Bereichen Aufklärung der Cyber-Bedrohung und Schutz kritischer Infrastrukturen: zur Aufklärung des Einsatzes, der Herkunft und der technischen Beschaffenheit der Cyber-Angriffsmittel sowie zur Gestaltung wirksamer Abwehrmassnahmen. Der Zweck der Funkaufklärung wird in der Verordnung über die elektronische Kriegsführung und die Funkaufklärung (VEKF, SR 510.292) konkretisiert. Demnach darf die Vorinstanz Funkaufklärungsaufträge ausschliesslich zur Beschaffung von sicherheitspolitisch bedeutsamen Informationen über Vorgänge im Ausland erteilen (Art. 3 Abs. 2 VEKF). Die zu beschaffenden Informationen müssen den Zielen gemäss Art. 3 Abs. 3 VEKF in den Bereichen Terrorismus, Proliferation, Spionageabwehr, ausländische Konflikte, Militär und Rüstung, Einsatzgebiete der Schweizer Armee, Cyber-Bedrohungen oder der Aufrechterhaltung und Weiterentwicklung der Beschaffungstätigkeiten der Vorinstanz und des Nachrichtendienstes der Armee dienen.

E. 9.3.1

Die beiden im Nachrichtendienstgesetz verwendeten Begriffe «sicherheitspolitisch bedeutsame Vorgänge im Ausland» und «weitere wichtige Landesinteressen» sind unbestimmt. Sie finden jedoch im Gesetz - in Art. 3 NDG - beziehungsweise auf Verordnungsebene - in Art. 25 NDV und Art. 3 Abs. 3 VEKF - eine (erste) verbindliche Konkretisierung. Das betrifft insbesondere den Begriff der sicherheitspolitisch bedeutsamen Vorgänge im Ausland. So konkretisieren die Verordnungen in Art. 25 NDV und Art. 3 Abs. 3 VEKF die Zweckrichtung der Informationsbeschaffung beziehungsweise die Tätigkeiten, die eine Informationsbeschaffung rechtfertigen. Der Verordnungsgeber verwendet jedoch wiederum unbestimmte Rechtsbegriffe wie «Terrorismus», «Proliferation», «gegen die Schweiz gerichtete Handlungen» oder «kritische Infrastrukturen». Eine Legaldefinition der Begriffe enthalten weder das Gesetz noch die Verordnungen.

E. 9.3.2

Bis zum Inkrafttreten des Nachrichtendienstgesetzes waren die Aufgaben der Vorinstanz teilweise im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120) geregelt. Zu den Aufgaben der Sicherheitsbehörden gehörte dabei unter anderem die Bekämpfung des Terrorismus. Soweit die zur Umschreibung des Aufgabenbereichs verwendeten Begriffe nicht bereits in anderen Erlassen definiert waren, verzichtete der Gesetzgeber bei Erlass des BWIS bewusst auf eine Legaldefinition. Zur Begründung wurde angegeben, dass sich die Erscheinungsformen der verschiedenen Bedrohungen ändern könnten (vgl. Botschaft vom 7. März 1994 zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und zur Volksinitiative «S.o.S. Schweiz ohne Schnüffelpolizei» [nachfolgend: Botschaft BWIS], BBl 1994 II 1127, 1128). Davon durfte der Gesetzgeber auch bei Erlass des Nachrichtendienstgesetzes ausgehen und den sachlichen Anwendungsbereich für die Funk- und Kabelaufklärung entsprechend relativ offen festlegen (vgl. in diesem Sinne auch das zit. Urteil Big Brother Watch und andere, §§ 370 f.; ferner die Botschaft NDG, BBl 2014 2105, 2143, die für den sachlichen Zuständigkeitsbereich auf das BWIS verweist).

E. 9.3.3

Ohnehin bleiben die verwendeten Begriffe trotz fehlender Legaldefinitionen nicht ohne Konturen. Die Materialien zum Nachrichtendienstgesetz verweisen im Zusammenhang mit dem sachlichen Anwendungsbereich auf das Bundesgesetz über die Wahrung der inneren Sicherheit (BWIS). Dieses enthielt selbst zwar, wie ausgeführt, ebenfalls keine Definition des Begriffs Terrorismus, aus den Materialien ergab sich jedoch eine Charakterisierung. Demnach handelt es sich um Terrorismus, wenn schwere Straftaten gegen Leib und Leben und die körperliche oder geistige Unversehrtheit angedroht oder verübt werden und hierfür ein politisches Motiv vorgebracht sowie eine bestimmte Strategie verfolgt wird (vgl. Botschaft BWIS, BBl 1994 II 1127, 1169). Zudem wird im Strafrecht und im Völkerrecht der Begriff der terroristischen Straftat verwendet (vgl. Art. 260quinquies StGB; Übereinkommen des Europarats zur Verhütung des Terrorismus vom 16. Mai 2005 [SR 0.311.61]; zur fehlenden völkerrechtlichen Definition von «Terrorismus» vgl. Deutscher Bundestag, Terrorismus als Gegenstand von Konzeptualisierungsversuchen, Entwicklungen in Politikwissenschaft und Völkerrecht seit 2001, WD 2 - 3000 - 002/23, 2023, < www.bundestag.de > Dokumente > Wissenschaftliche Dienste > Suchbegriff: Konzeptualisierungsversuch, abgerufen am 16. Oktober 2025). Weitere in Art. 25 NDV genannte Begriffe werden an anderer Stelle im Nachrichtendienstgesetz verwendet und

konkretisiert (vgl. Art. 6 Abs. 1 Bst. a Ziffn. 3 und 4 NDG für die Begriffe Proliferation und Schutz kritischer Infrastrukturen und Art. 19 Abs. 2 Bst. a NDG für den Begriff der terroristischen Aktivitäten) oder es ergibt sich eine inhaltliche Konkretisierung entweder aus der übrigen Rechtsordnung (vgl. Art. 265 ff. StGB betreffend die Verbrechen und Vergehen gegen den Staat und die Landesverteidigung) beziehungsweise aus der in der Verordnung formulierten Zweckrichtung (vgl. Art. 25 Bst. d NDV). Die Kabelaufklärung darf schliesslich nicht generell zur Beschaffung von Informationen über Vorgänge im Ausland eingesetzt werden (vgl. Wortlaut von Art. 6 Abs. 1 Bst. b NDG). Erforderlich ist vielmehr, dass es sich um sicherheitspolitisch bedeutsame Vorgänge handeln muss, mithin um solche, die sicherheitspolitisch für die Schweiz von einer gewissen Tragweite beziehungsweise Intensität sind.

E. 9.3.4

Die Vorinstanz stützt sich bei ihrer Arbeit und damit auch bei der Funk- und Kabelaufklärung zudem auf den sogenannten Grundauftrag; gemäss Art. 70 Abs. 1 NDG steuert der Bundesrat die Vorinstanz politisch und erteilt ihr hierzu periodisch einen Grundauftrag. Im Grundauftrag werden die Aufgaben der Vorinstanz gemäss Art. 6 NDG entsprechend der aktuellen sicherheitspolitischen Gegebenheiten konkretisiert. Eine zusammenfassende, als vertraulich bezeichnete Aktennotiz zum Grundauftrag, soweit dieser für die Funk- und Kabelaufklärung von Bedeutung ist, liegt dem Bundesverwaltungsgericht vor (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 7). Zudem verfügt die Vorinstanz über eine als vertraulich bezeichnete interne Dokumentation, in welcher die Begriffe unter anderem von Art. 6 NDG mit dem Ziel einer einheitlichen Begriffsverwendung definiert werden. Diese liegt dem Bundesverwaltungsgericht ebenfalls vor (Stellungnahme der Vorinstanz vom 11. November 2022, Anhang zu Beilage 7 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]) und konkretisiert die Begriffe auf der Grundlage des vorstehend dargestellten gesetzlichen Rahmens.

E. 9.3.5

Gemäss Art. 38 Abs. 2 Bst. b und Art. 39 Abs. 1 NDG können die Funk- und die Kabelaufklärung sodann zur Wahrung wichtiger Landesinteressen nach Art. 3 NDG eingesetzt werden. Hierfür ist ein Beschluss des Bundesrates gemäss Art. 71 NDG erforderlich (Botschaft NDG, BBl 2014 2105, 2140). Demnach kann der Bundesrat im Falle einer schweren und unmittelbaren Bedrohung die Vorinstanz mit Massnahmen nach diesem Gesetz beauftragen, sofern diese erforderlich sind, um weitere wichtige Landesinteressen nach Art. 3 NDG zu wahren. Der Bundesrat legt dabei im Einzelfall Dauer, Zweck, Art und Umfang der Massnahme fest (Art. 71 Abs. 2 NDG). Sollen auf der Grundlage eines entsprechenden Auftrags Informationen mittels Funk- oder Kabelaufklärung beschafft werden, ist das hierfür vorgesehen Verfahren einzuhalten (Botschaft NDG, BBl 2014 2105, 2140). Der Bestimmung von Art. 3 NDG kommt damit der Charakter einer Generalklausel zu, die im Falle einer schweren und unmittelbaren Bedrohung den Einsatz der Vorinstanz zum Schutz der Grundordnung der Schweiz (Bst. a), zur Unterstützung der Aussenpolitik (Bst. b) und zum Schutz des Werk-, Wirtschafts- und Finanzplatzes (Bst. c) zulässt.

E. 9.4

Die Funk- und die Kabelaufklärung dienen nach dem Gesagten der Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland. Ziel ist es, im

Zeitpunkt der Anordnung der Massnahmen noch unbekannte Bedrohungen etwa durch Terrorismus, die Verbreitung von Massenvernichtungswaffen oder für kritische Infrastrukturen aufzudecken. Die Art der Bedrohungen steht nicht von vornherein fest und kann sich im Verlaufe der Zeit verändern. Die relative Offenheit des Gesetzes (Art. 38 Abs. 2 und Art. 39 Abs. 1 i.V.m. Art. 3 und Art. 6 Abs. 1 Bst. b NDG) ist vor diesem Hintergrund als notwendig anzusehen und hinzunehmen. Ohnehin kann mit Blick auf das vorstehend Ausgeführte nicht gesagt werden, die Gründe, aus denen eine Massenüberwachung angeordnet werden darf, seien ohne ausreichend verbindliche Konturen. Zudem handelt es sich bei den in Art. 3, Art. 6 Abs. 1 Bst. b und Art. 38 Abs. 2 Bst. a NDG genannten Gründen, aus denen eine Funk- oder Kabelaufklärung angeordnet beziehungsweise genehmigt werden darf, um zulässige Eingriffszwecke im Sinne von Art. 8 Ziff. 2 und Art. 10 Ziff. 2 EMRK; sie sind der nationalen oder öffentlichen Sicherheit, dem wirtschaftlichen Wohl der Schweiz und der Aufrechterhaltung der Ordnung zuzurechnen. Aus dem Gesetz ergibt sich sodann in hinreichendem Mass, dass die Funk- und Kabelaufklärung nicht Selbstzweck sind; sie dienen der Beschaffung von Informationen über Vorgänge im Ausland, die für die Schweiz - aus unterschiedlichen Gründen (Art. 3, Art. 6 Abs. 1 Bst. b und Art. 38 Abs. 2 NDG) - von Interesse sind (vgl. in diesem Sinne ausdrücklich der Wortlaut von Art. 38 Abs. 2 Bst. a in fine NDG). Es ist mithin in hinreichendem Mass vorhersehbar, dass die Funk- und Kabelaufklärung auch und gerade Vorgänge im Ausland mit einem Bezug zur Schweiz betreffen kann (sog. Schweiz-Bezug), so etwa, wenn an einer Spionage oder Proliferation Personen im Inland beteiligt sind. Zweck der Funk- und Kabelaufklärung ist jedoch die Beschaffung von Informationen über Vorgänge im Ausland und der gesetzliche Rahmen (einschliesslich Massnahmen zum Schutz vor Missbrauch) ist darauf ausgerichtet. Vor diesem Hintergrund erscheint wichtig, dass der Fokus eines Auftrags zur Aufklärung auf einem Vorgang im Ausland liegt; die Herkunft der Informationen ist demgegenüber nicht entscheidend. Drauf weisen auch die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI und die Geschäftsprüfungsdelegation GPDel in ihren Jahresberichten hin (vgl. die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI, Jahresbericht 2023, im Original zu den Akten genommen als Beilage zum Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 30. Juli 2025 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 9. September 2025]; Geschäftsprüfungskommission und Geschäftsprüfungsdelegation der eidgenössischen Räte, Jahresbericht 2021 vom 25. Januar 2022, S. 123). Auf die Gefahr des Missbrauchs der Massenüberwachung im Zusammenhang mit Resultaten, die einen Schweiz-Bezug aufweisen, ist an anderer Stelle einzugehen (vgl. nachfolgend E. 16.3.4.3 und E. 21.2.2). Im Rahmen des ersten Prüfpunktes ist abschliessend von Bedeutung, dass mit der relativen Offenheit von Art. 38 Abs. 2 und Art. 39 Abs. 1 NDG die Gefahr von Missbrauch verbunden ist. Die relative Offenheit ist angesichts der zu regelnden Materie jedoch hinzunehmen. Es wird daher im Rahmen der gesamthaften Beurteilung zu prüfen sein, ob insgesamt ausreichende Garantien zum Schutz vor Missbrauch bestehen und daher die Informationsbeschaffung mittels Funk- und Kabelaufklärung insgesamt als notwendig beziehungsweise verhältnismässig angesehen werden kann. Im Vordergrund steht dabei die vorgängige Genehmigung durch eine unabhängige Behörde und deren konkretisierende Genehmigungspraxis (vgl. hierzu nachfolgend E. 13 f.; vgl. in diesem Sinne auch Hecker, a.a.O., III § 2 Rz. 35). Prüfpunkt 2 Umstände, unter denen die Kommunikation eines Individuums überwacht werden darf

E. 10

Zusätzlich zu den Gründen, aus denen eine Massenüberwachung genehmigt werden darf, müssen nach der Rechtsprechung des EGMR auch die Umstände, unter denen die Kommunikation überwacht werden darf, hinreichend bestimmt im Gesetz festgelegt sein. Der Gerichtshof erkennt dabei, dass die Massenüberwachung im Unterschied zur gezielten Überwachung - notwendigerweise - am Träger der Kommunikation ansetzt und nicht am einzelnen Gerät oder am Absender oder Empfänger einer Nachricht. Die Umstände, unter denen eine Kommunikation überwacht werden darf, können aus diesem Grund weiter gefasst sein als im Rahmen einer gezielten Überwachung (zit. Urteil Centrum för rättvisa, § 289). Der EGMR hatte in seinen beiden Urteilen Big Brother Watch und andere und Centrum för rättvisa die Regime zur Massenüberwachung des Vereinigten Königreichs und von Schweden zu überprüfen. In beiden Ländern war die Überwachung auf internationale Kommunikation beschränkt, das heisst auf Kommunikation über die Staatsgrenzen hinweg. Davon war auszugehen, wenn sich der Absender und/oder der Empfänger im Ausland befanden. Inländische Kommunikation, bei der sich Absender und Empfänger im Inland aufhielten, durfte nicht überwacht werden. Auf welchem Weg die Kommunikation übertragen wurde, war unerheblich; auch Kommunikation die von einem Absender im Inland über das Ausland an einen Empfänger im Inland geleitet wurde (sog. Inland-via Ausland-Kommunikation) galt als inländische Kommunikation (zit. Urteile Big Brother Watch und andere, §§ 373 f., und Centrum för rättvisa, § 290). Die Überwachungsbehörden waren vor diesem Hintergrund verpflichtet, möglichst diejenigen Informationsträger zu ermitteln, die internationale Kommunikation enthielten (vgl. zit. Urteil Big Brother Watch und andere, § 373). Dabei war unbestritten, dass eine Unterscheidung zwischen internationaler und inländischer Kommunikation (bereits beim Erfassen der Kommunikation) nicht immer möglich ist. Die Unterscheidung zwischen internationaler und inländischer Kommunikation konnte daher die Erfassung auch von interner Kommunikation nicht (in jedem Fall) verhindern. Die eigentliche Überwachung, das heisst die nachrichtendienstliche Verwertung von inländischer Kommunikation, war jedoch ausgeschlossen. Die betreffende Kommunikation musste vernichtet werden, sobald erkannt worden war, dass es sich um inländische Kommunikation handelt. Die Einschränkung auf internationale Kommunikation schränkt nach Ansicht des EGMR zudem, wenn auch in begrenztem Umfang, die Kategorie von Personen ein, deren Kommunikation überwacht werden darf und verhindert, dass die Regeln zur gezielten Überwachung von Personen im Inland umgangen werden. Der EGMR bezeichnete die Einschränkung auf internationale Kommunikation aus diesem Grund als eine Garantie zum Schutz vor Missbrauch durch ein Instrument der Massenüberwachung (zum Ganzen zit. Urteil Big Brother Watch und andere, §§ 372-375). Der Gerichtshof hielt schliesslich fest, dass weder der Absender noch der Empfänger einer Nachricht den Weg der Übertragung bestimmen können. Die Umstände, unter denen die Kommunikation überwacht werden darf, konnten aus diesem Grund generell-abstrakt nicht weiter eingegrenzt werden. Der EGMR sah aus diesem Grund in beiden Fällen die Umstände, unter denen die Kommunikation einer Person abgehört werden könne, als hinreichend vorhersehbar an (vgl. zit. Urteile Big Brother Watch und andere, § 376, und Centrum för rättvisa, § 294).

E. 11.1

Gemäss Art. 39 Abs. 1 NDG kann die Vorinstanz den durchführenden Dienst im Rahmen einer Kabelaufklärung damit beauftragen, zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland sowie zur Wahrung weiterer wichtiger Landesinteressen grenzüberschreitende Signale aus leitungsgebundenen Netzen

zu erfassen. Befindet sich sowohl der Sender als auch der Empfänger in der Schweiz, so ist die Verwendung der erfassten Signale nach Absatz 1 nicht zulässig. Kann der durchführende Dienst solche Signale nicht bereits bei der Erfassung ausscheiden, so sind die beschafften Daten (Inhalts- und Randdaten) zu vernichten, sobald erkannt wird, dass sie von solchen Signalen stammen (Art. 39 Abs. 2 NDG). Gemäss den Materialien stellt die Bestimmung von Art. 39 Abs. 2 NDG sicher, dass keine rein schweizerische Kommunikation erfasst wird. Wo dies nicht möglich ist, weil der Leitweg von «IP-Datenpaketen» nicht vorhergesagt werden kann, sind solche Daten unverzüglich zu vernichten, sobald ihre schweizerische Herkunft und Zieladresse erkannt werden. Diese Verpflichtung trifft sowohl die Vorinstanz als auch den Beigeladenen als durchführenden Dienst (Botschaft NDG, BBl 2014 2105, 2179).

E. 11.2.1

Die Vorinstanz und der Beigeladene äussern sich insbesondere im Rahmen ihrer Antworten zu den Fragenkatalogen des Bundesverwaltungsgerichts zur Umsetzung der Vorgaben gemäss Art. 39 Abs. 1 und 2 NDG in der Praxis zur Kabelaufklärung.

E. 11.2.2

Gemäss Art. 39 Abs. 1 kann die Vorinstanz den Beigeladenen mit der Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland beauftragen. Die Beschaffung entsprechender Informationen ist mithin Sache des Beigeladenen (vgl. Art. 42 NDG und Art. 26 NDV). Für die nachrichtendienstliche Auswertung hingegen ist die Vorinstanz zuständig (Art. 42 Abs. 5 NDG). Zur Beschaffung der Informationen durch Kabelaufklärung würden zunächst diejenigen Fernmeldedienstanbieterinnen ausgewählt, die über eigene leitungsgebundene Netze verfügten, die zudem der Übertragung grenzüberschreitender Signale dienten. Unter einem Signal sei dabei der Träger der Information zu verstehen, im Falle beispielsweise einer Glasfaser also das optische Signal. Ein Signal sei sodann grenzüberschreitend, wenn es physisch oder logisch ins Ausland übermittelt wird; der Beigeladene nimmt eine funktionale Betrachtungsweise ein und geht von grenzüberschreitenden Signalen immer dann aus, wenn sich zumindest ein Adressierungselement im Ausland befindet. Entsprechend könnten etwa auch Peering-Leitungen im Inland von Bedeutung für die Kabelaufklärung sein, wenn auf diesen in relevantem Mass logisch grenzüberschreitende Signale übermittelt werden (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 2 ff. [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]; Stellungnahme des Beigeladenen vom 11. April 2025, S. 7; Stellungnahme des Beigeladenen vom 19. Januar 2024, S. 5). Zur Auswahl relevanter Fernmeldedienstanbieterinnen führt der Beigeladene gemäss den Ausführungen der Vorinstanz technische Abklärungen bei beziehungsweise über Fernmeldedienstanbieterinnen mit Sitz in der Schweiz durch; die technischen Parameter sind dem Bundesverwaltungsgericht bekannt, sie werden jedoch von der Vorinstanz als vertraulich bezeichnet. Die Fernmeldedienstanbieterinnen hätten zudem gegenüber dem Beigeladenen technische Angaben zu machen. Gestützt auf diese Abklärungen und Angaben entscheide die Vorinstanz, ob der Fernmeldeverkehr der Anbieterin von Interesse für eine Kabelaufklärung sei. Dabei sei es nicht möglich, vorab abschliessend zu beurteilen, ob eine Leitung tatsächlich zur Übermittlung von Signalen ins Ausland verwendet werde; das Gesetz sehe keine Testerfassung von Signalen vor. Sei eine Leitung Gegenstand eines Auftrags zur Kabelaufklärung, werde jeweils der gesamte Datenverkehr erfasst, wobei die Erfassung nur in eine Richtung erfolge, also beispielsweise

bei der Übermittlung der Kommunikation ins Ausland. Dabei sei nicht erforderlich, dass alle Signale grenzüberschreitend seien. Die Kabelaufklärung dürfe auch Leitungen einbeziehen, über die neben Signalen ins Ausland auch rein schweizerische Kommunikation übertragen werde (sog. gemischter Verkehr; Stellungnahme des Beigeladenen vom 11. April 2025, S. 6 f.). Nach der Anbindung einer Fernmeldedienstanbieterin erfolge die Erfassung der Signale auf der Sicherungsschicht (Layer 2 gemäss dem OSI-Modell). Im Rahmen der technischen Umsetzung einer Kabelaufklärung erhalte der Beigeladene alsdann Zugriff auf eine Kopie der betreffenden Signale (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 4 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]).

E. 11.2.3

Gemäss Art. 39 Abs. 2 NDG ist die Verwendung der erfassten Signale nicht zulässig, wenn sich sowohl der Sender als auch der Empfänger in der Schweiz befinden (sog. rein schweizerische Kommunikation; vgl. Botschaft NDG, BBl 2014 2105, 2179). Für die Beurteilung, ob sich der Sender und/oder der Empfänger in der Schweiz befinde, stelle der Beigeladene darauf ab, ob sich diese - und sei es nur temporär - örtlich in der Schweiz aufhalten. Gemäss den weiteren Ausführungen der Vorinstanz und des Beigeladenen ist es technisch nicht möglich, etwa gestützt auf eine Filterung der Randdaten der Kommunikation rein schweizerische Kommunikation in jedem Fall bei der Übertragung beziehungsweise Erfassung auszuscheiden, insbesondere, wenn es sich um sogenannte Inland-via Ausland-Kommunikation beispielsweise über einen Server im Ausland handelt. Bei einer Kabelaufklärung werde daher auch rein schweizerische Kommunikation, die auf Leitungen mit gemischtem Verkehr verlaufe, miterfasst (Stellungnahme der Vorinstanz vom 11. April 2025, S. 5; Stellungnahme der Vorinstanz vom 11. Juli 2023, S. 4 f.; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 4 ff.). Nach der Erfassung setze der Beigeladene verschiedene automatische Filter ein. Die erfassten Signale würden in der Regel auf der Netzwerk- beziehungsweise Vermittlungsschicht (Layer 3 gemäss dem sog. Open Systems Interconnection-Modell [OSI-Modell]) ein erstes Mal automatisch gefiltert. Konkret werde geprüft, ob die Randdaten der Kommunikation eine IP-Adresse enthalten, die sich laut Geolokalisierung in der Schweiz befindet. Gegebenenfalls würden die Signale entsprechend markiert. Die Signale würden sodann aufbereitet und auf der Anwendungsschicht (Layer 7 gemäss dem OSI-Modell) anhand weiterer Merkmale (Schweizer Telefonnummer, Schweizer IBAN-Nummer, Schweizer Adresse) inhaltlich gefiltert. Seien die Daten nicht vollständig und könnten Herkunft und Inhalt nicht rekonstruiert werden, würden die Daten gelöscht und das Löschen werde protokolliert. Ergebe die Filterung einen Bezug zur Schweiz, würden die Daten ebenfalls markiert. Gleichzeitig werde unerwünschte Kommunikation ausgeschieden. Hierfür werde die erfasste Telekommunikation automatisch nach bestimmten Dateiformaten gefiltert. Anschliessend würden die verbleibenden Inhalts- und Verbindungsdaten (einschliesslich der markierten Kommunikationen) durch Anwendung spezifischer Selektoren durchsucht. In einem letzten Schritt würden die Resultate von einer Analystin oder einem Analysten des Beigeladenen überprüft. Ergebe sich im Rahmen dieser Überprüfung, dass es sich um eine rein schweizerische Kommunikation handelt, würden die betreffenden Daten vernichtet. Die Daten würden nicht der Vorinstanz weitergeleitet - anders als Daten aus der sogenannten Inland-Ausland-Kommunikation, bei der sich nur entweder der Absender oder der Empfänger in der Schweiz befinde (vgl. Art. 39 Abs. 2 und Art. 42 Abs. 2 NDG). In sehr wenigen Fällen - die Vorinstanz nennt in ihrer Stellungnahme vom 11. November 2022

insgesamt zwei Fälle - ist es vorgekommen, dass eine rein schweizerische Kommunikation nicht erkannt und die Daten an die Vorinstanz weitergeleitet worden sind (Stellungnahme des Beigeladenen vom 8. März 2024, S. 5 ff.; Stellungnahme des Beigeladenen vom 19. Januar 2024, S. 6 f.; Stellungnahme der Vorinstanz vom 11. Juli 2023, S. 17, 19 und 21 f.: Stellungnahme des Beigeladenen vom 10. November 2022, S. 7-10; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 4 ff. und S. 11 f.).

E. 11.3

Die Schranke gemäss Art. 39 Abs. 2 NDG ist auch Gegenstand der Kontrolle der Tätigkeit der Vorinstanz durch die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI; die Kontrollinstanz untersucht die Resultate der Funk- und Kabelaufklärung stichprobenweise (Art. 10 Abs. 1 Bst. d VAND). Sie erstattet dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport VBS jährlich Bericht über ihre Prüfungen (Art. 10 Abs. 3 VAND; vgl. zum Verfahren und zu den Modalitäten für die Kontrolle durch eine unabhängige Behörde nachfolgend E. 19-21). Dem Bundesverwaltungsgericht liegen die Berichte über die Prüfungen der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI für die Jahre 2019 - 2024 im Original vor. Die Kontrollinstanz bezeichnet die Berichte als vertraulich; die Berichte enthalten Angaben zu Aufklärungsaufträgen und zum Vorgehen von Vorinstanz und Beigeladenen sowie zu Ergebnissen der Kabelaufklärung und damit auch zu deren Effektivität. Für sie gilt daher grundsätzlich der Quellenschutz gemäss Art. 35 NDG. Die Kontrollinstanz hat dem Bundesverwaltungsgericht vor diesem Hintergrund die Berichte zusätzlich in teilweise geschwärzter Form eingereicht. Das Bundesverwaltungsgericht hat den Beschwerdeführenden die teilweise geschwärzten Berichte der Kontrollinstanz zugestellt und ihnen im Übrigen gestützt auf Art. 28 VwVG den wesentlichen Inhalt der geschwärzten Textpassagen bekannt gegeben (vgl. hierzu vorstehend Sachverhalt Bst. Y.a und E. 7.6.3). Die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI führt jährlich vier Inspektionsbesuche bei der Vorinstanz und einen Kontrollbesuch beim Beigeladenen durch. Ein Schwerpunkt der Untersuchungen sind die Aufklärungsprodukte mit einem Bezug zur Schweiz; die Kontrollinstanz lässt sich vom Beigeladenen zeigen, wie die Kommunikation mit einem Bezug zur Schweiz identifiziert und - bei rein schweizerischer Kommunikation - ausgesondert wird. Gemäss den Jahresberichten hat die Anzahl Aufklärungsprodukte, die einen Bezug zur Schweiz aufweisen und aus diesem Grund anonymisiert wurden (Art. 42 Abs. 2 NDG), über die Jahre deutlich abgenommen.

E. 11.4.1

Aus dem Gesetz (Art. 39 Abs. 1 und Abs. 2 NDG) ergibt sich, dass zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland im Rahmen einer Kabelaufklärung grenzüberschreitende Signale aus leitungsgebundenen Netzen erfasst werden dürfen. Zudem wird die Verwendung der erfassten Signale eingeschränkt. Sie ist nicht zulässig, wenn sich sowohl der Sender als auch der Empfänger in der Schweiz befinden. Damit ist grundsätzlich vorhersehbar, dass die Kabelaufklärung bei der grenzüberschreitenden Kommunikation ansetzt. Zwar ist allein gestützt auf das Gesetz nicht ohne Weiteres erkennbar, dass auch sogenannte Inland-via Ausland-Kommunikation erfasst wird. Diesbezüglich schafft jedoch Art. 39 Abs. 2 NDG Klarheit: Die Erfassung rein schweizerischer Kommunikation soll vermieden werden. Für den Fall, dass gleichwohl rein schweizerische Kommunikation beziehungsweise Inland-via Ausland-Kommunikation erfasst wird, ist die Verwendung der erfassten Signale nicht zulässig und die betreffenden

Daten sind zu vernichten, sobald erkannt wird, dass sie von solchen Signalen stammen. Grundsätzlich und unter Berücksichtigung des zu prüfenden Sachverhalts sind damit die Umstände, unter denen die Kommunikation überwacht werden darf, in hinreichendem Mass vorhersehbar (vgl. im Ergebnis auch BGE 144 I 126 E. 6.2).

E. 11.4.2

Die Beschwerdeführenden sind demgegenüber der Ansicht, dass die Kabelaufklärung nicht zielgerichtet auf grenzüberschreitende Kommunikation ausgerichtet werden könne. Im Rahmen der Kabelaufklärung werde daher in erheblichem Umfang auch rein schweizerische Kommunikation erfasst. Die Beschränkung der Kabelaufklärung auf grenzüberschreitende Signale habe mithin in Wirklichkeit keine limitierende Wirkung und biete keinen wirksamen Schutz vor Missbrauch. Zudem bleibe insgesamt unklar, was Vorinstanz und Beigeladener unter einem grenzüberschreitenden Signal verstünden. Zur Begründung verweisen die Beschwerdeführenden auf die technischen Besonderheiten der Übertragung von Kommunikation über das Internet. So lasse sich weder bestimmen noch vorhersagen, über welche «Route» Signale beziehungsweise Datenpakete im Internet übertragen würden. Die Übertragung erfolge dynamisch und hänge unter anderem davon ab, wie die einzelnen Anbieterinnen von Fernmeldedienstleistungen (im Rahmen eigener autonomer Systeme) miteinander verbunden seien und welche Kapazitäten im Moment der Übertragung bestünden. Zudem könnten die einzelnen Provider lediglich über die oberste Datenschicht, das heisst die Bitübertragungsschicht (sog. Physical Layer bzw. Layer 1 gemäss dem OSI-Modell), nicht jedoch über die eigentliche Adressierung (IP-Adresse auf Layer 3 gemäss dem OSI-Modell) Auskunft geben. Aus diesen Gründen sei es nicht möglich, im Voraus Leitungen zu bestimmen, die (überwiegend) zur Datenübertragung ins Ausland, sei es physisch oder logisch, genutzt würden. Hinzu komme, dass beispielsweise die Kommunikation via E-Mail in der Regel serverbasiert erfolge. Eine Nachricht werde vom Absender zunächst an den Server des betreffenden Providers und damit regelmässig ins Ausland übermittelt, selbst wenn es sich um eine rein schweizerische Kommunikation handelt. Auch solche Kommunikation werde erfasst, wobei offen bleibe, wie der Beigeladene erkennen könne, ob sich etwa eine Person, die eine E-Mail-Adresse mit der Domain gmail.com nutze, in der Schweiz aufhalte. Zwar führten Vorinstanz und Beigeladene an, mittels der sogenannten Geolokalisierung könne rein schweizerische Kommunikation und auch Kommunikation mit einem Bezug zur Schweiz erkannt und markiert werden. Die Geolokalisierung sei jedoch angesichts der paketvermittelten und häufig serverbasierten Kommunikation, die zudem im Zusammenspiel verschiedener Provider und auf der Grundlage eines hochdynamischen Routings erfolge, nicht zuverlässig. Zudem würden die Signale - entgegen der Angaben der Vorinstanz und des Beigeladenen - mittels Splitting nicht erst auf der Sicherungsschicht, sondern bereits auf der Bitübertragungsschicht (Layer 1 gemäss dem OSI-Modell), ausgeleitet beziehungsweise erfasst, wobei auf dieser Schicht nicht unterschieden werden könne, ob es sich um ein grenzüberschreitendes oder ein inländisches Signal handle; das weitere Routing und damit der Empfänger einer Nachricht sei erst auf der Vermittlungsschicht (Layer 3 gemäss OSI-Modell) festgelegt. Das Verständnis, das die Vorinstanz und der Beigeladene dem Begriff des grenzüberschreitenden Signals beigeben würde, führe dazu, dass potentiell alle Übertragungsleitungen und damit die gesamte über das Internet geführte Kommunikation von der Kabelaufklärung erfasst werde. Damit bleibe der Begriff beziehungsweise die Einschränkung der Kabelaufklärung auf grenzüberschreitende Signale letztlich ohne hinreichende Konturen und begrenze die Kabelaufklärung nicht effektiv. Die unzureichende

Vorhersehbarkeit führe zu einem chilling effect. Schliesslich weisen die Beschwerdeführenden auf die extraterritoriale Wirkung der Garantien gemäss der EMRK hin, wonach auch Personen im Ausland in den persönlichen Schutzbereich der hier betroffenen Garantien fielen. Die betroffenen Personen hätten mithin dieselben Ansprüche wie Personen im Inland. Unterschiedliche Schutzniveaus seien nicht zulässig.

E. 11.4.3

Die Rechtsprechung geht davon aus, dass bei der Erfassung von grenzüberschreitenden Signalen eine Unterscheidung von rein inländischer Kommunikation von der Kommunikation mit Bezug zum Ausland (Sender oder Empfänger befindet sich im Ausland) technisch nicht (immer) möglich ist, umso mehr, als die Kommunikationsdaten nicht in jedem Fall den Standort des Senders und/oder Empfängers preisgeben. Zudem kann nicht ohne Weiteres vorab bestimmt werden, welche Leitungen für die Übermittlung tatsächlich grenzüberschreitender Kommunikation (entweder der Sender oder der Empfänger oder sowohl der Sender und der Empfänger befinden sich im Ausland) verwendet werden (vgl. auch vorstehend E. 11.2.2; zudem den zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Rz. 26 ff. und Rz. 165; zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, Rz. 170 ff.; Erläuternder Bericht Revision NDG zu Art. 42 Abs. 3bis; ferner die «partly concurring and partly dissenting opinion» von Richter Pinto de Albuquerque zum zit. Urteil Big Brother Watch und andere, §§ 8 f. und 38 ff., insbes. §§ 40 und 43). Das ist hier im Wesentlichen mit Blick auf die Inland-via Ausland-Kommunikation von Bedeutung. Auch der Gesetzgeber verlangt (vor diesem Hintergrund) nicht, dass entsprechende Kommunikation in keinem Fall erfasst werden darf. Er schreibt vielmehr vor, dass die Verwendung nicht zulässig ist, wenn sich sowohl der Sender als auch der Empfänger in der Schweiz befindet. Und kann der Beigeladene 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). Das deutsche Bundesverfassungsgericht hielt in seinem Beschluss zur sogenannten Inland-Ausland-Aufklärung gestützt auf Angaben der deutschen Bundesregierung fest, dass der deutsche Bundesnachrichtendienst ein elektronisches Filterfahren zur Erkennung rein inländischer Kommunikation führt, das auf der Grundlage metadatenbezogener Indizien und Parameter funktioniere. Damit könnten bis zu 98 % der rein inländischen Kommunikation erkannt werden (zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Rz. 29 f.). Auch der Beigeladene verwendet ein solches elektronisches Filterverfahren. Zwar ist die Effizienz mangels entsprechender Angaben nicht konkret bekannt, doch kann aufgrund der Ausführungen des deutschen Bundesverfassungsgerichts auch nicht gesagt werden, einem solchen Verfahren ginge von vornherein jede Zwecktauglichkeit zur Markierung und späteren Ausscheidung von rein schweizerischer Kommunikation ab. Weiter geht aus den dem Bundesverwaltungsgericht vorliegenden Informationen nicht klar hervor, ob der Beigeladene markierte Signale beziehungsweise Daten automatisch vernichtet oder ob dies erst nach der Analyse durch einen Mitarbeitenden des Beigeladenen erfolgt. Ist letzteres der Fall, würde dies die Beeinträchtigung der berührten Grundrechte erhöhen, da die Daten inhaltlich nicht mehr nur automatisch, sondern durch einen Analysten beurteilt würden. Von entscheidender Bedeutung ist dies jedoch hier nicht. Der Gesetzgeber hat die Tätigkeiten der Informationsbeschaffung und der nachrichtendienstlichen Auswertung sowie Verwendung getrennt; zuständig für die Informationsbeschaffung ist der Beigeladene, während die

nachrichtendienstliche Auswertung und Verwendung der gewonnenen Informationen Sache der Vorinstanz ist (vgl. Art. 42 Abs. 1 und Abs. 5 NDG; Art. 26 NDV). Selbst wenn also rein schweizerische Kommunikation nicht bereits bei der Erfassung ausgeschieden werden kann, so ist durch die elektronische Filterung und eine (allfällige) Analyse der (markierten) Signale und Daten in hinreichendem Mass sichergestellt, dass rein inländische Kommunikation nicht für die nachrichtendienstliche Auswertung durch die Vorinstanz verwendet wird. Damit wird die Kabelaufklärung in ihrer Reichweite erheblich eingeschränkt; insbesondere ist in hinreichendem Mass ausgeschlossen, dass mittels der Kabelaufklärung die einschränkende Regelung zur direkten Überwachung von Personen im Inland umgangen werden kann.

E. 11.4.4

Die Umstände, unter denen die Kommunikation der Beschwerdeführenden im Rahmen einer Kabelaufklärung überwacht werden darf, sind somit nach den Umständen hinreichend vorhersehbar. Zudem bieten der Umstand, dass der Beigeladene nicht unmittelbar Zugriff auf die Fernmeldeübertragung hat - er erhält lediglich Signalkopien -, das Verwendungsverbot rein schweizerischer Kommunikation und die Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung in zweckmässiger Weise Schutz vor Missbrauch. Weiter kann nicht gesagt werden, die Praxis von Vorinstanz und Beigeladenem führe dazu, dass die Konventionsrechte von Personen im Ausland verletzt würden. Schweizer Behörden verfügen im Ausland über keine Hoheitsbefugnisse, so dass Erkenntnisse in der Regel für Betroffene nicht unmittelbar mit Folgen verbunden sind. Es ist daher sachlich gerechtfertigt, nur rein schweizerische Kommunikation von der Verwendung auszuschliessen und im Übrigen eine nachrichtendienstliche Auswertung zuzulassen (vgl. zur Anonymisierungspflicht bezüglich Informationen über Personen im Inland Art. 42 Abs. 2 NDG und nachfolgend E. 16.2.1 und E. 16.3.4.3). Da zudem der Weg, auf dem Kommunikation im Internet übertragen wird, nicht im Voraus bestimmt werden kann, können die Umstände, unter denen die Kommunikation der Beschwerdeführenden überwacht werden darf, kaum weiter eingegrenzt werden als generell und mit Blick auf das Ziel der Überwachung und das Verbot, rein schweizerische Kommunikation für die nachrichtendienstliche Auswertung zu verwenden (vgl. in diesem Sinne auch das zit. Urteil Big Brother Watch und andere, § 376; zur Verwendung besonders schützenswerter Kommunikation zudem nachfolgend E. 15.2 und E. 16.3.6). Unerheblich ist schliesslich, bei wem die Kommunikationen im Rahmen einer Kabelaufklärung erfasst werden; die Beschwerdeführenden weisen darauf hin, dass die Vorinstanz von Fernmeldedienstanbieterinnen spreche, während das Gesetz in Art. 43 NDG Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsdienstleistungen erwähne. Die Umstände, unter denen die Kommunikation der Beschwerdeführenden überwacht werden darf, sind mit der Einschränkung auf die Verwendung grenzüberschreitender Signale und den Ausschluss rein inländischer Kommunikation in hinreichendem Mass vorhersehbar.

E. 11.5

Mit der laufenden Revision des Nachrichtendienstgesetzes soll der Beigeladene neu die Möglichkeit erhalten, die im Rahmen von bestehenden Aufträgen erfassten Signale und Daten technisch zu analysieren mit dem Ziel, technische Angaben über Datenströme zu gewinnen. Hierzu soll im Gesetz in Art. 42 NDG ein neuer Abs. 3bis eingeführt werden mit folgendem Wortlaut (Vernehmlassungsvorlage zur Revision des Bundesgesetzes vom 25.

September 2015 über den Nachrichtendienst, < www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2022 > VBS, abgerufen am 16. Oktober 2025): 3bis Der durchführende Dienst kann im Rahmen von bestehenden Aufträgen erfasste Signale und Daten analysieren, um technische Angaben über Datenströme zu gewinnen, die er nicht von den Betreiberinnen von leitungsgebundenen Netzen und den Anbieterinnen von Telekommunikationsdienstleistungen erhalten kann. Der NDB kann diese Erkenntnisse für die Formulierung der Anträge verwenden. Die neu zu schaffende Möglichkeit der technischen Analyse erfasster Signale und Daten wird damit begründet, dass die Anbieterinnen von Fernmeldedienstleistungen wider Erwarten nicht in der Lage seien, hinreichende Auskünfte über die von ihnen geführten internationalen Datenströme zu machen; sie würden - worauf auch die Beschwerdeführenden hinweisen - in der Regel nur die Herkunfts- und Zielpunkte der Datenströme in den benachbarten Ländern, nicht jedoch die weiterreichende Herkunft und auch nicht die Endpunkte kennen. Hintergrund sei unter anderem das hochdynamische Routing. Dem Beigeladenen soll es daher neu möglich sein, die erfassten Signale und Daten technisch zu analysieren, um ein möglichst aktuelles und realitätsgetreues Bild der bearbeiteten Datenströme, der damit transportierten Signale und der Herkunft und Destination der Kommunikationen zu erhalten. Zudem soll die «technische Beschaffenheit» der Daten ermittelt werden. Diese Art der Auswertung sei nicht auf den Informationsgehalt der erfassten Signale bezogen, sondern technischer Natur; Ziel sei es, zu erkennen, «wo welche Arten von Datenströmen transportiert werden und welche davon nachrichtendienstlich relevante Informationen enthalten können». Gewonnene Erkenntnisse würden beim Beigeladenen gespeichert, könnten jedoch mit der Vorinstanz zwecks Formulierung neuer Aufträge geteilt werden (Erläuternder Bericht Revision NDG zu Art. 42 Abs. 3bis). Die zu schaffende Möglichkeit der technischen Analyse von erfassten Kommunikationen und Randdaten stellt eine Beeinträchtigung des durch Verfassung und EMRK geschützten Privatbereichs dar. Diese wiegt jedoch nicht besonders schwer (vgl. vorstehend E. 6.3.2). Zusätzlich fällt hier die Trennung von Informationsbeschaffung durch den Beigeladenen und nachrichtendienstlicher Auswertung und Verwendung von Erkenntnissen durch die Vorinstanz in Betracht. Die allfällige Möglichkeit der technischen Analyse erscheint daher nicht von vornherein als nicht vereinbar mit Verfassung und EMRK. Es wäre jedoch sicherzustellen, dass die technische Analyse auch personell getrennt von der Analyse im Rahmen der Funk- und Kabelaufklärung erfolgt.

E. 12.1

Gemäss Art. 38 Abs. 1 NDG kann der Bund sodann einen Dienst für die Erfassung elektromagnetischer Ausstrahlungen von Telekommunikationssystemen, die sich im Ausland befinden, betreiben (sog. Funkaufklärung). Sie dient der Beschaffung von sicherheitspolitisch bedeutsamen Informationen über Vorgänge im Ausland; Daten über Personen und Vorgänge im Inland, die als solche erkannt worden sind, müssen vom Beigeladenen grundsätzlich vernichtet werden (Art. 5 VEKF). Die Funkaufklärung ist gemäss den Materialien auf das Ausland ausgerichtet; es dürfen nur Funksysteme, die sich im Ausland befinden, erfasst werden. In der Praxis betrifft dies vor allem Telekommunikationssatelliten, die Funksignale auch über dem Gebiet der Schweiz abstrahlen, und Kurzwellensender, wie sie etwa im Bereich des Flugverkehrs oder vom Militär verwendet werden (Botschaft NDG, BBl 2014 2105, 2177).

E. 12.2

Aus dem Gesetz und den Materialien ergibt sich, dass im Rahmen der Funkaufklärung mit entsprechenden Empfangsanlagen in der Schweiz Funksignale aufgefangen werden, die von Telekommunikationssatelliten und Kurzwellensendern auch auf das Gebiet der Schweiz abgestrahlt werden. Damit sind die Umstände, unter denen die Kommunikation (der Beschwerdeführenden) im Rahmen der Funkaufklärung überwacht werden darf, nach den Umständen hinreichend vorhersehbar. Zwar sieht das anwendbare Recht im Unterscheid zur Kabelaufklärung nicht vor, dass rein schweizerische Kommunikation nicht verwendet werden darf und - sobald erkannt - zu vernichten ist. Aus Gesetz und Verordnung ergibt sich jedoch (immerhin), dass die Funkaufklärung der Beschaffung von sicherheitspolitisch relevanten Informationen im Ausland mit Auswirkungen auf die Schweiz dient und Daten über Vorgänge im Inland grundsätzlich zu vernichten sind (zur Anonymisierungspflicht bezüglich Informationen über Personen im Inland Art. 38 Abs. 4 Bst. b NDG und nachfolgend E. 16.2.1 und E. 16.3.4.3). Damit erfährt die Funkaufklärung im Hinblick auf die Umstände, unter denen die Kommunikation überwacht werden darf, eine hinreichende Einschränkung. Prüfpunkt 3 Das für die Erteilung der Genehmigung einzuhaltende Verfahren

E. 13.1

Im Rahmen des dritten Prüfpunktes ist zu unterscheiden zwischen der Beeinträchtigung des Privatlebens (Art. 13 BV und Art. 8 EMRK) und der Beeinträchtigung der Medienfreiheit (Art. 17 BV und Art. 10 EMRK); der EGMR verlangt zum Schutz journalistischer Quellen besondere Garantien gegen Missbrauch. Vor diesem Hintergrund ist im Folgenden zunächst auf die Anforderungen einzugehen, die der EGMR zum Schutz des Privatlebens an ein Regime zur Massenüberwachung stellt (nachfolgend E. 13.2). Hiernach ist auf die besonderen Garantien einzugehen, die erforderlich sind, um eine Beeinträchtigung der Medienfreiheit rechtfertigen zu können (nachfolgend E. 13.3).

E. 13.2.1

Der EGMR geht im Zusammenhang mit der Massenüberwachung in Bezug auf den Schutz des Privatlebens gemäss Art. 8 EMRK von einem immanenten Missbrauchsrisiko aus. Er verlangt daher in seiner Rechtsprechung durchgehende Garantien («garanties de bout en bout» bzw. «end-to-end-safeguards»; zit. Urteil Big Brother Watch und andere, § 350 [Hervorhebungen nur hier]): [...], la Cour considère qu'afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, le processus doit être encadré par des « garanties de bout en bout », c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ - dès la définition de l'objet et de l'étendue de l'opération - et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré a posteriori. Ces facteurs sont, de l'avis de la Cour, des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8 [...]. Zur Genehmigung durch eine unabhängige Instanz hält die Grosse Kammer des EGMR im Allgemeinen fest, dass eine richterliche Genehmigung eine wichtige Garantie gegen Missbrauch ist, sie jedoch kein notwendiges Erfordernis darstellt. Jedenfalls sollte die Massenüberwachung durch ein von der Exekutive unabhängiges Organ genehmigt werden. Um einen wirksamen Schutz vor Missbrauch zu gewährleisten, ist das unabhängige Organ sodann über den Zweck der Überwachung und die vermutlich zu überwachenden Übertragungsleitungen beziehungsweise Kommunikationswege zu

informieren. Dies ermöglicht es der Behörde, die Notwendigkeit und damit die Verhältnismässigkeit der Massenüberwachung und im Konkreten auch der Auswahl der Träger der Kommunikation zu beurteilen (zit. Urteil Big Brother Watch und andere, §§ 351 f.).

E. 13.2.2

Der EGMR bezeichnet im Weiteren die Verwendung von Selektoren und insbesondere von starken Selektoren als einen der wichtigsten Schritte im Prozess der Massenüberwachung, da dies der Punkt ist, an dem die Kommunikation eines bestimmten Individuums anvisiert werden kann; starke Selektoren sind Suchbegriffe, die mit identifizierbaren Personen im Zusammenhang stehen, also etwa Namen, Telefonnummern oder E-Mail-Adressen. Dabei akzeptiert der Gerichtshof mit Blick auf die Charakteristika einer Massenüberwachung - die Überwachung der internationalen Kommunikation ausserhalb der Hoheitsgewalt des Staates, eine grosse Zahl an verwendeten Selektoren und ein immanentes Bedürfnis nach Flexibilität bei der Auswahl der Selektoren -, dass eine abschliessende Nennung der zulässigen Selektoren nicht verlangt werden kann. Die Genehmigung sollte jedoch zumindest die Arten oder Kategorien der zu verwendenden Selektoren bezeichnen (vgl. zit. Urteil Big Brother Watch und andere, §§ 353 f.). Für starke Selektoren, die mit identifizierbaren Individuen in Zusammenhang stehen, sind zudem verstärkte Garantien anzuwenden; die Notwendigkeit und damit die Verhältnismässigkeit der Verwendung ist zu begründen, die Rechtfertigung zu dokumentieren und die Verwendung einem Verfahren vorheriger (interner) Genehmigung zu unterwerfen (zit. Urteil Big Brother Watch und andere, § 355; zum Ganzen auch zit. Urteil Centrum för rättvisa, §§ 265-269).

E. 13.2.3

Im zitierten Urteil Centrum för rättvisa hatte die Grosse Kammer des EGMR das damalige schwedische Regime der Massenüberwachung von grenzüberschreitender elektronischer Kommunikation zu beurteilen. Dieses schrieb für das Genehmigungsverfahren die Beteiligung eines Datenschutzbeauftragten («un représentant chargé de la protection de la vie privée» bzw. «a privacy protection representative») vor. Damit sollte dem Umstand begegnet werden, dass aus Gründen der Geheimhaltung das Genehmigungsverfahren nicht öffentlich durchgeführt wurde. Der Datenschutzbeauftragte handelte im öffentlichen Interesse. Er hatte Zugang zu allen Unterlagen und konnte Erklärungen abgeben. Die Genehmigung wurde zudem von einem von der Exekutive unabhängigen Gericht erteilt, das den Bedarf an den gewünschten Erkenntnissen, die Kommunikationsträger, zu denen um Zugang ersucht wurde, und die Selektoren, die eingesetzt werden sollten, prüfte und genehmigte. Der Eingriff in das Recht auf Privatleben musste zudem so weit wie möglich begrenzt werden. Der Gerichtshof bezeichnete schliesslich den Umstand, dass die Entscheidungen des Gerichts bindend waren und in einem Verfahren mit Beteiligung eines Datenschutzbeauftragten getroffen wurden, als wichtigen Schutz, der in das schwedische Regime der Massenüberwachung eingebaut worden war (vgl. zit. Urteil Centrum för rättvisa, §§ 297-299).

E. 13.3

Eine Beeinträchtigung der Medienfreiheit gemäss Art. 10 EMRK kann nach der Rechtsprechung des EGMR nur gerechtfertigt sein, wenn sie mit hinreichenden Verfahrensgarantien einhergeht. Diese sollen gewährleisten, dass eine Beeinträchtigung der Medienfreiheit nur im Falle eines überwiegenden öffentlichen Interesses gerechtfertigt

werden kann. Jede Anordnung oder Massnahme, die zu einer Offenlegung journalistischer Quellen führt, muss daher von einer unabhängigen Behörde überprüft werden (können). Diese muss zudem befugt sein, vor der Herausgabe der Informationen zu entscheiden, ob ein überwiegendes öffentliches Interesse besteht, das den Grundsatz des Schutzes der Quellen von Journalisten überwiegt, und, falls dies nicht der Fall ist, jeden nicht unbedingt erforderlichen Zugang zu Informationen zu verhindert, der zur Offenlegung der Identität einer Quelle führen könnte (vgl. zit. Urteil Big Brother Watch und andere, §§ 444 f. unter Verweis auf das Urteil des EGMR [Grosse Kammer] Sanoma Uitgevers B.V. gegen die Niederlande vom 14. September 2010, 38224/03, §§ 88-90). In seinem Urteil Big Brother Watch und andere entwickelte der EGMR den dargestellten Ansatz für den Bereich der Massenüberwachung weiter. Demnach ist mit der Verwendung von Suchbegriffen, die mit einem Journalisten in Verbindung stehen (sog. starke Selektoren), die Gefahr verbunden, dass erhebliche Mengen an vertraulichem journalistischem Material beschafft werden. Damit würde der Schutz journalistischer Quellen untergraben. Der Gerichtshof verlangt daher im Zusammenhang mit der durch die Bundesverfassung und die EMRK geschützte Medienfreiheit beziehungsweise den Schutz journalistischer Quellen folgende Garantie zum Schutz vor Missbrauch (zit. Urteil Big Brother Watch und andere, § 448): [...] En conséquence, la Cour estime qu'avant que les services de renseignement ne puissent utiliser des sélecteurs ou des termes de recherche dont on sait qu'ils sont liés à un journaliste ou qui aboutiront en toute probabilité à la sélection pour examen d'éléments journalistiques confidentiels, ces sélecteurs ou termes de recherche doivent avoir été autorisés par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si cette mesure est « justifiée par un impératif prépondérant d'intérêt public » et, en particulier, si une mesure moins intrusive suffirait à satisfaire un tel impératif ([...]).

E. 14.1

Aufträge zur Kabelaufklärung sind gemäss Art. 40 Abs. 1 NDG genehmigungspflichtig. Bevor die Vorinstanz einen Auftrag zur Kabelaufklärung erteilt, holt sie die Genehmigung des Bundesverwaltungsgerichts sowie die Freigabe durch die Vorsteherin oder den Vorsteher des Departementes für Verteidigung, Bevölkerung und Sport VBS ein (Art. 40 Abs. 2 NDG; vgl. für die Freigabe auch Art. 40 Abs. 3 NDG). Das Genehmigungsverfahren richtet sich grundsätzlich nach den für die genehmigungspflichtigen Beschaffungsmassnahmen geltenden Bestimmungen von Art. 29-32 NDG (Art. 41 Abs. 2 NDG). In Art. 41 NDG sind die Anforderungen an einen Antrag auf Genehmigung und die Geltungsdauer einer Genehmigung beziehungsweise die Möglichkeit einer Verlängerung der Genehmigung speziell für die Kabelaufklärung geregelt. Gemäss Art. 41 Abs. 1 NDG hat ein Antrag zur Genehmigung einer Kabelaufklärung eine Beschreibung des Auftrags (Bst. a), die Begründung der Notwendigkeit des Einsatzes (Bst. b), die Kategorien von Suchbegriffen (Bst. c), Angaben zu den Betreiberinnen von leitungsgebundenen Netzen und den Anbieterinnen von Telekommunikationsdienstleistungen, welche die für die Durchführung der Kabelaufklärung notwendigen Signale liefern müssen (Bst. d) sowie Angaben zu Beginn und Ende des Auftrags (Bst. e) zu enthalten. 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 Sätze 2 und 3 NDG). Der Umstand, dass mit der Genehmigung Kategorien von Suchbegriffen festgelegt werden, ermöglicht es, die Suchbegriffe dynamisch zu handhaben und im Verlaufe der Kabelaufklärung - gestützt auf erste Ergebnisse - zu verfeinern (Botschaft NDG, BBl 2014 2105, 2179 f.). Zuständig für

die Beurteilung und Genehmigung eines Antrags auf Genehmigung eines Auftrags zur Kabelaufklärung ist das Bundesverwaltungsgericht (Art. 40 Abs. 2 NDG; Art. 36b des Verwaltungsgerichtsgesetzes [VGG, SR 173.32]). Gemäss Art. 29 Abs. 2 NDG entscheidet die Präsidentin oder der Präsident der zuständigen Abteilung beziehungsweise ein mit dieser Aufgabe betrauter anderer Richter mit kurzer Begründung innerhalb von fünf Arbeitstagen nach Erhalt des Antrags als Einzelrichter; das Bundesverwaltungsgericht hat hierfür organisatorisch in der Abteilung I ein eigenes Fachgebiet, das sogenannte Fachgebiet NDG, geschaffen. Im Rahmen der Entscheidfindung kann die Anhörung von Vertreterinnen und Vertretern der Vorinstanz angeordnet werden (Art. 29 Abs. 4 NDG) und die Genehmigung kann mit Auflagen erteilt werden (Art. 29 Abs. 5 NDG). Die Genehmigung gilt sodann für höchstens sechs Monate. Sie kann nach demselben Verfahren um jeweils höchstens drei Monate verlängert werden (Art. 41 Abs. 3 NDG). Das Verfahren für die Freigabe eines Auftrags zur Kabelaufklärung ist in Art. 30 NDG geregelt. Gemäss Art. 32 Abs. 1 NDG beendet die Vorinstanz einen Auftrag zur Kabelaufklärung unter anderem dann, wenn die Frist abgelaufen ist (Bst. a) oder die Voraussetzungen für eine weitere Durchführung nicht mehr erfüllt sind (Bst. b). Mit der Genehmigung werden, wie ausgeführt, die zulässigen Suchbegriffe nach Kategorien genehmigt. Gemäss Art. 27 Abs. 4 NDV kann der Beigeladene der Vorinstanz vorschlagen, im Rahmen der genehmigten und freigegebenen Kategorien zusätzliche Suchbegriffe in laufende Aufträge aufzunehmen. Diese Suchbegriffe können auch aus Erkenntnissen aus anderen Aufträgen, namentlich der Funkaufklärung, hervorgehen. Die Funkaufklärung steht, anders als die Kabelaufklärung, unter keinem Genehmigungsvorbehalt; sie wird von der Vorinstanz in eigener Verantwortung eingesetzt (vgl. Art. 3 Abs. 1 VEKF; vorstehend E. 5.3).

E. 14.2.1

Die Vorinstanz äussert sich im Rahmen ihrer Rechtsschriften insbesondere zu den Angaben, die im Antrag auf Genehmigung zu den Kategorien von Suchbegriffen zu machen sind. Sie hat dem Bundesverwaltungsgericht zudem eine Liste der Kategorien von Suchbegriffen zu den (damals) laufenden Kabelaufklärungsaufträgen eingereicht; die Liste enthält auszugsweise die Anträge zu den (damals) laufenden Aufträgen zur Kabelaufklärung, einschliesslich Angaben zur Orientierung und zum Bedürfnis sowie zu den Kategorien von Suchbegriffen (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 4). Die Liste ist als geheim bezeichnet. Die Vorinstanz legt dar, dass sie in ihren Anträgen um Genehmigung eines Auftrags zur Kabelaufklärung die Kategorien von Suchbegriffen zum besseren Verständnis jeweils auf eine sogenannte Orientierung und ein sogenanntes Bedürfnis bezieht. Die Orientierung enthalte Angaben zum thematischen Rahmen und zum Hintergrund beziehungsweise Anlass des Auftrags, während das Bedürfnis das nachrichtendienstliche Interesse (vgl. hierzu insbes. Art. 25 NDV) und damit die Zweckrichtung eines Auftrags zur Kabelaufklärung konkretisiere. Mit der Orientierung und dem Bedürfnis solle sichergestellt werden, dass der Auftrag und damit die Suchbegriffe einen hinreichenden nachrichtendienstlichen Bezug aufweisen (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 11). Auf diese Weise gäben die Orientierung und das Bedürfnis den Analysten des Beigeladenen den thematischen Rahmen des jeweiligen Auftrags zur Kabelkaufklärung vor (Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 3 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Als Kategorien von Suchbegriffen dienten Oberbegriffe wie «natürliche Personen». Dadurch, dass diese Begriffe in Beziehung gesetzt würden zur Orientierung und zum Bedürfnis, werde der Rahmen des jeweiligen Auftrags

zur Kabelaufklärung eingeschränkt beziehungsweise konkretisiert. Die auszugsweise eingereichten und als vertraulich bezeichneten Anträge enthalten für jede Kategorie von Suchbegriffen zudem beispielhaft eine Aufzählung konkreter Suchbegriffe (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 4). Die konkreten Suchbegriffe würden laufend an neue Erkenntnisse angepasst. Diese Möglichkeit steht sowohl der Vorinstanz selbst als auch dem Beigeladenen (Art. 27 Abs. 4 NDV) zu, wobei der Beigeladene Suchbegriffe, die den bisher verwendeten Begriffen sehr nahe sind, selbständig anwenden dürfe (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 6 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Neue Suchbegriffe müssten sich inhaltlich den vom Bundesverwaltungsgericht genehmigten Kategorien von Suchbegriffen zuordnen lassen können. Die Aufnahme zusätzlicher Suchbegriffe in eine Kabelaufklärung werde im Informationssystem Kommunikationsaufklärung (ISCO), das der Kontrolle und der Steuerung der Funk- und Kabelaufklärung dient (Art. 56 Abs. 1 NDG), dokumentiert. Für jeden erfassten Suchbegriff werde zudem eine Referenznummer zum entsprechenden Auftrag zur Kabelaufklärung im Informationssystem der Geschäftsverwaltung (GEVER NDB), der Zeitpunkt der Beauftragung und eine Identifikation des Auftraggebenden und des Beauftragten festgehalten (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 10 und 11). Suchbegriffe seien in ihrer Art schliesslich nicht auf Wörter beschränkt; als Suchbegriff könne auch eine Kombination von Zahlen und/oder Buchstaben (z.B. eine Telefonnummer) dienen (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 11). Für die Beurteilung, ob es sich bei Angaben um solche einer schweizerischen natürlichen oder juristischen Person handelt, die nicht als Suchbegriff verwendet werden dürfe, stellt die Vorinstanz auf die Staatsbürgerschaft und den Aufenthaltsort beziehungsweise den Sitz ab (vgl. zur Auskunfts- und Meldepflicht von Behörden gegenüber der Vorinstanz Art. 20 NDG; mit der laufenden Gesetzesrevision soll der Begriff «schweizerische natürliche oder juristische Personen» durch den Begriff «natürliche oder juristische Personen im Inland ersetzt werden, womit künftig auf den Aufenthaltsort beziehungsweise Sitz abgestellt würde und Angaben über alle Personen in der Schweiz als Suchbegriff nicht zulässig wären [vgl. vorstehend E. 4.3.3 und Erläuternder Bericht Revision NDG zu Art. 39 NDG]).

E. 14.2.2

Das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) äussert sich im Rahmen seiner Antworten zu den Fragenkatalogen insbesondere zu seinem Prüfprogramm bei der Genehmigung von Aufträgen zur Kabelaufklärung. Demnach prüft das Bundesverwaltungsgericht zunächst, ob sich ein Auftrag zur Kabelaufklärung auf sicherheitspolitisch bedeutsame Vorgänge - im Sinne einer grösseren Entwicklung - im Ausland bezieht; die Kabelaufklärung dürfe nicht für die Erkenntnisgewinnung hinsichtlich einzelner Personen eingesetzt werden und sei auch kein Mittel zur Inlandaufklärung, wobei entsprechende Informationen innerhalb der Grenzen gemäss Art. 42 Abs. 3 NDG verwendet werden dürften. Weiter werde für einen Auftrag zur Kabelaufklärung vorausgesetzt, dass die betroffenen Betreiberinnen und Anbieterinnen von Fernmeldedienstleistungen mitwirkungspflichtig im Sinne des Gesetzes seien. Und schliesslich werde geprüft, ob der Auftrag zur Kenntniserlangung notwendig und verhältnismässig sei. Hierfür sei erforderlich, dass die Kabelaufklärung geeignet sei, im konkreten Aufklärungsbereich relevante Informationen zu liefern. In diesem Sinne seien auch die von der Aufklärung betroffenen Leitungen und die Kategorien von Suchbegriffen festzulegen. Schliesslich

müsse - im Sinne des Verhältnismässigkeitsgrundsatzes - ein Auftrag zur Kabelaufklärung thematisch und geographisch hinreichend eingeschränkt sein (Stellungnahme des Bundesverwaltungsgerichts [Abteilung I, Fachgebiet NDG] vom 12. Oktober 2022, S. 3-5). Das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) merkt sodann zur Erstgenehmigung an, dass die Kategorien von Suchbegriffen in der Praxis sehr weit gefasst seien und kaum Suchbegriffe denkbar seien, die sich nicht darunter subsumieren liessen. Der Prüfung der Kategorien von Suchbegriffen komme daher kaum eine beschränkende Wirkung zu. Zudem könne bei der Erstbeurteilung eines Auftrags zur Kabelaufklärung dessen Notwendigkeit nur schwer abgeschätzt werden; konkrete Produkte und deren nachrichtendienstlicher Mehrwert liessen sich kaum antizipieren. Die Notwendigkeit eines Auftrags zur Kabelaufklärung könne nach der Erfahrung des Bundesverwaltungsgerichts (Abteilung I, Fachgebiet NDG) zweckmässig erst nach dessen Implementierung anhand der gewonnenen Resultate beurteilt werden (Stellungnahme des Bundesverwaltungsgerichts [Abteilung I, Fachgebiet NDG] vom 12. Oktober 2022, S. 4). Das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) verlangt in der Praxis, dass einem Gesuch um Verlängerung eines Auftrags zur Kabelaufklärung die bisherigen Resultate aus der Kabelaufklärung beizulegen und der nachrichtendienstliche Mehrwert der Resultate auszuweisen ist. Bei der Beurteilung eines Gesuchs um Verlängerung prüfe das Bundesverwaltungsgericht sodann vorfrageweise die Rechtmässigkeit der bisher gewonnenen Resultate. Konkret werde beurteilt, ob das Resultat unter Beachtung von Art. 39 Abs. 3 NDG auf einem rechtmässigen Suchbegriff beruhe, ob sich das Resultat (hauptsächlich) auf einen sicherheitspolitisch bedeutsamen Vorgang im Ausland beziehe und nachrichtendienstlich einen Mehrwert aufweise. Bezüglich des Mehrwerts sei die Vorinstanz darlegungspflichtig, wobei «Standardfloskeln» nicht ausreichen würden. Vielmehr habe die Vorinstanz bei jedem Resultat das Aufklärungsziel detailliert zu beschreiben, die konkreten Erkenntnisse, die das Resultat betreffend dieses Ziel liefere, zu erläutern und schliesslich schlüssig darzulegen, weshalb diese Erkenntnisse nachrichtendienstlich wertvoll seien. Bei Bedarf stelle das Bundesverwaltungsgericht Ergänzungsfragen (Stellungnahme des Bundesverwaltungsgerichts [Abteilung I, Fachgebiet NDG] vom 12. Oktober 2022, S. 4 f.; Stellungnahme des Bundesverwaltungsgerichts [Abteilung I, Fachgebiet NDG] vom 24. Oktober 2023, S. 2). Die zulässigen Resultate würden alsdann in einem nächsten Schritt in die Beurteilung eines Gesuchs um Verlängerung eines Auftrags zur Kabelaufklärung einbezogen. Hierbei, also bei der Beurteilung eines Gesuchs um Verlängerung eines Auftrags, sei wiederum gesamthaft die Verhältnismässigkeit der Massnahme (Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinn) zu prüfen (Stellungnahme des Bundesverwaltungsgerichts [Abteilung I, Fachgebiet NDG] vom 12. Oktober 2022 S. 5 f.). Im Zusammenhang mit der Pflicht zur Begründung von Entscheiden über die Genehmigung gemäss Art. 29 Abs. 2 NDG hält das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) fest, dass sich das Gericht im ersten Laufjahr eines Auftrags eine gewisse Zurückhaltung auferlege; Genehmigungsverfügungen würden summarisch begründet. Nach dem ersten Laufjahr finde bei jeder Verlängerung eine umfassende Prüfung statt und die Begründung könne unter Umständen sehr umfangreich sein (Stellungnahme des Bundesverwaltungsgerichts [Abteilung I, Fachgebiet NDG] vom 12. Oktober 2022, S. 6). In grundsätzlicher Weise hält das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) schliesslich fest, mit der Kabelaufklärung sei insbesondere aufgrund von deren Heimlichkeit, der grossen Streubreite und der fehlenden Mitteilungspflicht ein «gewichtiger» Eingriff in das grundrechtlich

geschützte Privatleben verbunden. Es weist zudem auf die Möglichkeit hin, dass der Beigeladene unter bestimmten Umständen - einer konkreten Bedrohung der inneren Sicherheit - Informationen über Personen im Inland der Vorinstanz auf entsprechenden Antrag hin in nicht anonymisierter Form bekannt gibt (sog. Entanonymisierung). Dies könne zur Folge haben, dass schweizerische Personen aufgrund einer strategischen Überwachung, für die keine konkrete Bedrohungslage vorausgesetzt sei (vgl. im Unterscheid hierzu Art. 27 Abs. 1 Bst. a NDG betreffend die sog. genehmigungspflichtigen Beschaffungsmassnahmen), zum Ziel weiterer Massnahmen der schweizerischen Behörden würden (Stellungnahme des Bundesverwaltungsgerichts [Abteilung I, Fachgebiet NDG] vom 12. Oktober 2022, S. 5 f.).

E. 14.3

Gemäss Art. 29 Abs. 8 NDG erstellt die Präsidentin oder der Präsident der für die Genehmigung zuständigen Abteilung des Bundesverwaltungsgerichts einen jährlichen Tätigkeitsbericht zuhanden der Geschäftsprüfungsdelegation (GPDel). Der Instruktionsrichter ersuchte das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) unter Hinweis auf den Rückweisungsentscheid des Bundesgerichts um Edition der betreffenden Tätigkeitsberichte ersucht. Das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) verwies diesbezüglich auf die Geschäftsprüfungsdelegation (GPDel), da die Berichte zu deren Handen erstellt würden. Mit Schreiben vom 11. August 2023 lehnte die Geschäftsprüfungsdelegation (GPDel) eine Edition der Tätigkeitsberichte ab mit der Begründung, diese seien einzig für die Geschäftsprüfungsdelegation (GPDel) als parlamentarische Oberaufsicht bestimmt. Es wies sodann darauf hin, dass dieser Entscheid abschliessend sei und auch für das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) gelte. Das Bundesverwaltungsgericht nimmt die Beurteilung unter Prüfpunkt 3 gestützt auf die verfügbaren Hinweise zur Genehmigungspraxis des Bundesverwaltungsgerichts (Abteilung I, Fachgebiet NDG) vor.

E. 14.4.1

Aus der vorstehend dargestellten Rechtsprechung des EGMR ergeben sich die wesentlichen Kriterien, nach denen das Verfahren bei der Erteilung der Genehmigung zu beurteilen ist: - Genehmigungsvorbehalt - Unabhängigkeit der Genehmigungsbehörde - Verbindlichkeit der Entscheidung - Festlegung der Suchbegriffe (nach Kategorien) - zeitliche Befristung der Genehmigung Anhand insbesondere dieser Kriterien ist im Folgenden zu prüfen, ob das anwendbare Recht in Bezug auf die Funk- und Kabelaufklärung hinreichende und wirksamen Garantien zum Schutz vor Missbrauch enthält. Einzugehen ist dabei zunächst auf die Kabelaufklärung.

E. 14.4.2

Gemäss Art. 40 Abs. 2 NDG hat die Vorinstanz, bevor sie einen Auftrag zur Kabelaufklärung erteilt, die Genehmigung des Bundesverwaltungsgerichts einzuholen (vgl. auch Art. 40 Abs. 1 NDG). Aufträge zur Kabelaufklärung stehen mithin unter einem Genehmigungsvorbehalt. Zudem ist mit der Zuständigkeit des Bundesverwaltungsgerichts auch das Erfordernis der Unabhängigkeit der Genehmigungsbehörde von der Exekutive erfüllt (vgl. Art. 2 VGG). Ein Antrag auf Genehmigung muss sodann eine Beschreibung des Auftrags enthalten und es sind die Kategorien von Suchbegriffen anzugeben. Das Bundesverwaltungsgericht prüft gestützt auf diese Angaben praxisgemäss, ob der Auftrag für einen der im Gesetz genannten Zwecke erteilt werden soll und ob dieser notwendig und

verhältnismässig ist. Zwar ist im Gesetz nicht ausdrücklich festgehalten, dass Entscheide des Bundesverwaltungsgerichts verbindlich sind. Die Verbindlichkeit der Entscheidungen ergibt sich jedoch implizit aus Art. 40 Abs. 2 NDG, wonach die Genehmigung einzuholen ist, bevor ein Auftrag zur Kabelaufklärung erteilt wird. Die Genehmigung ist schliesslich zeitlich in hinreichendem Mass befristet; sie gilt für höchstens sechs Monate und kann um jeweils höchstens drei Monate verlängert werden (vgl. das zit. Urteil Ekimdzhiev und andere, § 305, in welchem der EGMR ausgeführt hat, eine Gültigkeitsdauer von zwei Jahren verbunden mit den unklaren Konturen des Begriffs der nationalen Sicherheit schwäche die vorgängige gerichtliche Kontrolle erheblich). Das Verfahren zur Erteilung der Genehmigung eines Auftrags zur Kabelaufklärung enthält damit grundsätzlich hinreichende Garantien zum Schutz vor Missbrauch, insbesondere, da die Genehmigung ex ante durch das Bundesverwaltungsgericht und damit durch eine von der Verwaltung unabhängige Instanz erteilt wird (vgl. zu den Anforderungen an ein Gericht i.S.v. Art. 30 Abs. 1 und Art. 191c BV sowie Art. 6 Ziff. 1 EMRK BGE 151 I 93 E. 2.1.1; zum Erfordernis eine Genehmigung ex ante vgl. auch BGE 140 I 381 E. 4.5.2 f.). Eine gerichtliche Überprüfung ist die beste Garantie für die Unabhängigkeit, die Unparteilichkeit und ein ordentliches Verfahren. Daran ändert nichts, dass das Verfahren zur Genehmigung eines Auftrags zur Kabelaufklärung seine inhärenten Grenzen hat, auf die das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) hinweist; gemäss dem Bundesverwaltungsgericht kann die Beurteilung eines Auftrags zur Kabelaufklärung im ersten Laufjahr aufgrund von dessen Ausgestaltung als ein Instrument der präventiven Auslandsaufklärung lediglich mit eingeschränkter Prüfungsdichte erfolgen und es kommt der Bezeichnung der Kategorien von Suchbegriffen nur in eingeschränktem Mass eine begrenzende Funktion zu (vgl. in diesem Sinn auch die Ausführungen der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI in den Berichten über ihre Prüfungen, im Original zu den Akten genommen mit Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 5. Oktober 2022, 7. September 2023 und 30. Juli 2025; ferner Isenring/Quiblier, a.a.O., S. 136). Im Weiteren ist mit Blick auf das zwingende Erfordernis der Geheimhaltung insbesondere in der Phase der Erstgenehmigung und der Durchführung der Kabelaufklärung auch die Einschränkung an Transparenz beziehungsweise Öffentlichkeit des Genehmigungsverfahrens zu akzeptieren (vgl. in diesem Sinne auch das zit. Urteil Centrum för rättvisa, § 297). Hervorzuheben ist ferner, dass das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) eine Verlängerung der Genehmigung praxisgemäss jeweils gestützt auf die konkreten Resultate überprüft, wobei die einem Gesuch um Verlängerung beigelegten Resultate vorab auf ihre Rechtmässigkeit hin beurteilt werden. Zudem wird dadurch, dass die Aufnahme und Verwendung von zusätzlichen Selektoren einschliesslich einer Begründung dokumentiert wird, die Verwendung von Selektoren für die Genehmigungs- und die Überwachungsbehörde überprüfbar gemacht; die Überprüfbarkeit ergibt sich dabei unter anderem aus der Verknüpfung der Suchbegriffe mit einer Orientierung und einem Bedürfnis (vgl. hierzu auch BGE 149 I 218 E. 8.7.2). Die Praxis der gerichtlichen ex ante-Beurteilung von Genehmigungsanträgen, die insofern umfassend ist, als das Ziel des Einsatzes, die betroffenen Betreiberinnen von leitungsgebundenen Netzen und die Kategorien der zu verwendenden Selektoren kontrolliert werden, bietet somit insgesamt einen bedeutenden Schutz gegen missbräuchliche oder eindeutig unverhältnismässige Überwachungsmassnahmen. Dabei ist wichtig, dass das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) jeweils prüft, ob ein Auftrag zur Kabelaufklärung

(weiterhin) einen Vorgang im Ausland betrifft und nicht (schleichend) zu einem Instrument der Inlandsaufklärung wird (vgl. hierzu auch vorstehend E. 9.4). Das anwendbare Recht enthält jedoch keine Regelung im Zusammenhang mit der Genehmigung von starken Selektoren und aus den Ausführungen der Vorinstanz und des Bundesverwaltungsgerichts (Abteilung I, Fachgebiet NDG) lässt sich diesbezüglich auch keine gesonderte Praxis entnehmen. Zwar sind Angaben über schweizerische natürliche und juristische Personen als Suchbegriffe nicht zulässig (Art. 39 Abs. 3 Satz 3 NDG), was mit Blick auf die Zweckrichtung der Kabelaufklärung geboten erscheint. Angaben zu Personen im Ausland und damit auch zu Journalisten oder etwa Rechtsanwälten, deren Kommunikation mit Mandanten besonders schützenswert ist (vgl. vorstehend E. 6.2.1 und 6.3.3), dürfen hingegen als Suchbegriffe verwendet werden (vgl. hierzu kritisch Rainer J. Schweizer, Völkerrechtliche Schranken internationaler nachrichtendienstlicher Aktivitäten, Aktuelle Juristische Praxis [AJP] 2017 S. 1096, der die Einschränkung auf Personen im Ausland als völkerrechtswidrig bezeichnet). Die Unterscheidung zwischen Personen im Inland und solchen im Ausland lässt sich mit Blick auf die im Ausland fehlenden hoheitlichen Befugnisse der Behörden grundsätzlich sachlich begründen (vgl. hierzu auch vorstehend E. 6.3.4). An dieser Stelle ist allerdings in Betracht zu ziehen was folgt: Im Genehmigungsverfahren sind lediglich die Kategorien von Suchbegriffen anzugeben. Gemäss der Rechtsprechung des EGMR ist dies aus Gründen unter anderem der Flexibilität zwar hinzunehmen. Zum Ausgleich der widerstreitenden Interessen verlangt der Gerichtshof jedoch, dass die Verwendung starker Suchbegriffe im Hinblick auf Notwendigkeit und Verhältnismässigkeit gerechtfertigt werden muss. Diese Rechtfertigung muss genau dokumentiert und einem Verfahren vorheriger interner Genehmigung unterworfen werden, das eine gesonderte und objektive Beurteilung ermöglicht (zit. Urteil Big Brother Watch und andere, §§ 355 und 383). Die Verwendung von Suchbegriffen, von denen bekannt ist, dass sie mit einem Journalisten in Verbindung stehen, muss zudem von einem Richter oder einer einem anderen von der Vorinstanz unabhängigen und unparteiischen Entscheidungsgremium genehmigt werden (vgl. zit. Urteil Big Brother Watch und andere, § 456). Zwar verfügt hier der Beigeladene über eine interne, als vertraulich bezeichnete Weisung zur Selbstkontrolle personenbezogener Suchbegriffe, gemäss welcher personenbezogene Suchbegriffe mit einer Beschreibung und Begründung zu versehen sind, um eine periodische Kontrolle (alle zwei Wochen) zu ermöglichen, wobei die Kontrollen zu dokumentieren sind (Stellungnahme des Beigeladenen vom 8. März 2024, Beilage 1 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Dabei handelt es sich jedoch nur - aber immerhin - um eine interne Regelung des Beigeladenen zur (nachträglichen) Selbstkontrolle. Die Hürde einer formellen vorgängigen Genehmigung durch eine (andere beziehungsweise vorgesetzte) interne Stelle für das Verwenden von starken Suchbegriffen wird damit aber nicht erreicht. Das Fehlen einer Regelung zur internen beziehungsweise unabhängigen Genehmigung von starken Suchbegriffen stellt insbesondere mit Blick auf besonders schützenswerte Kommunikationen einen Mangel im Verfahren dar. Ob dieser Mangel durch andere Garantien etwa im Zusammenhang mit dem Verfahren die Auswahl, Auswertung und Verwendung des abgefangenen Materials (Prüfpunkt 4) oder durch die Kontrolle durch eine unabhängige Behörde (Prüfpunkt 7) ausgeglichen werden kann, ist im Rahmen der abschliessenden Gesamtbeurteilung zu prüfen. Das hier anwendbare Recht sieht schliesslich - anders als das damals geltende schwedische Recht, das im zitierten Urteil Centrum för rättvisa zu beurteilen war - nicht vor, dass ein Datenschutzbeauftragter oder eine andere

fachkundige, im öffentlichen Interesse handelnde Person am Genehmigungsverfahren beteiligt ist. Ein Ausgleich der widerstreitenden Interessen ist daher hier im Verfahren zur Genehmigung eines Auftrags zur Kabelaufklärung nicht in gleichem Mass gewährleistet; während das öffentliche Interesse an der Informationsbeschaffung durch die Vorinstanz vertreten wird, bleibt das (öffentliche) Interesse an der Einhaltung der gesetzlichen Schranken der Informationsbeschaffung ohne Vertretung. Da als Genehmigungsbehörde mit dem Bundesverwaltungsgericht ein unabhängiges Gericht eingesetzt ist, fällt dieser Umstand im Rahmen des dritten Prüfpunktes nicht entscheidend ins Gewicht. Die Teilnahme eines Datenschutzbeauftragten am Genehmigungsverfahren stellt jedoch eine wirksame Massnahme zum Schutz vor Missbrauch dar (vgl. zit. Urteil Centrum för rättvisa, §§ 297 und 299) und es ist im Rahmen der Gesamtbeurteilung darauf zurückzukommen (vgl. nachfolgend E. 25).

E. 14.4.3

Mit der laufenden Gesetzesrevision soll die Dauer, während der eine Genehmigung für eine Kabelaufklärung gültig ist, von sechs auf zwölf Monate ausgedehnt werden. Zudem könnte die Genehmigung anstatt für drei neu für höchstens sechs Monate verlängert werden. Begründet wird dies mit der strategischen und damit längerfristigen Ausrichtung der Kabelaufklärung und dem grossen Aufwand für die Erarbeitung eines Antrags um Verlängerung (Erläuternder Bericht Revision NDG zu Art. 41 Abs. 3). Gemäss den Angaben des Bundesverwaltungsgerichts (Abteilung I, Fachgebiet NDG) kann bei der Erstbeurteilung eines Auftrags zur Kabelaufklärung dessen Notwendigkeit nur schwer abgeschätzt werden. Die Beurteilung erfolge daher im Rahmen der Erstgenehmigung nur mit eingeschränkter Prüfungsdichte. Auch wenn es sich dabei um eine inhärente Grenze des Genehmigungsverfahrens handelt, darf nicht ausser Acht bleiben, dass mit der Kabelaufklärung insbesondere aufgrund von deren Streubreite eine schwere Beeinträchtigung von Grundrechten verbunden ist. Es erscheint daher erforderlich, die Gültigkeit einer Genehmigung wie bisher zeitlich auf sechs Monate zu befristen. Auf diese Weise wird nach sechs Monaten im Rahmen eines Gesuchs um Verlängerung wenn auch noch keine umfassende, so aber doch eine erste Überprüfung der Kabelaufklärung auf der Grundlage von (ersten) Resultaten ermöglicht. Zur Begrenzung des behördlichen Ermessens und unter Berücksichtigung des mit der Kabelaufklärung verbundenen Eingriffs in das durch Bundesverfassung und EMRK geschützte Privatleben ist eine solche zeitliche Begrenzung notwendig. Eine weitere Überprüfung nach jeweils sechs weiteren Monaten im Rahmen eines Gesuchs um Verlängerung erscheint indes grundsätzlich verhältnismässig.

E. 14.4.4

Die Funkaufklärung steht im Gegensatz zur Kabelaufklärung nicht unter dem Vorbehalt der Genehmigung durch eine unabhängige Behörde. Dies dürfte im Wesentlichen darauf zurückzuführen sein, dass die für die Kabelaufklärung geltende Genehmigungspflicht im Wesentlichen auf der notwendigen Beteiligung schweizerischer Anbieterinnen von Fernmeldedienstleistungen gründet (vgl. hierzu vorstehend E. 6.3.4) und dieser Umstand bei der Funkaufklärung entfällt. Auch die Funkaufklärung ist jedoch ein Instrument zur Massenüberwachung und beeinträchtigt dergestalt das durch Bundesverfassung und EMRK geschützte Privatleben. Indem es vorliegend an einem Genehmigungsvorbehalt fehlt - die Vorinstanz erteilt Aufträge zur Funkaufklärung grundsätzlich in eigener Verantwortung - besteht kein Schutz ex ante gegen missbräuchliche Überwachungsmassnahmen. Dies fällt insbesondere deshalb besonders ins Gewicht, da geheimen Überwachungsmassnahmen der

Ausschluss des individuellen vorherigen Rechtsschutzes immanent ist und damit eine wichtige rechtsstaatliche und praxisbildende Kontrolle entfällt (vgl. in diesem Sinne auch das zitierte Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung Rz. 278). Als Folge des fehlenden Genehmigungsvorbehalts besteht auch keine besondere Prüfpflicht in Bezug auf starke Selektoren. Ob dieser grundlegende Mangel im Hinblick auf die ebenfalls fehlende zeitliche Beschränkung durch eine effektive und fortlaufende Kontrolle (zumindest) gemindert werden kann, wird im Rahmen der abschliessenden gesamthaften Prüfung zu beurteilen sein.

E. 14.5.1

Zusammenfassend ist betreffend die Kabelaufklärung zunächst festzuhalten, dass das Verfahren zur Erteilung der Genehmigung eines Auftrags zur Kabelaufklärung bedeutenden Schutz gegen Missbrauch bietet. Dieser ergibt sich zunächst daraus, dass mit dem Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) ein unabhängiges Gericht verbindlich über die Genehmigung entscheidet und dabei insbesondere auch die Kategorien von Suchbegriffen festlegt. Die Genehmigung ist zudem zeitlich auf sechs Monate befristet mit der Möglichkeit um Verlängerung, wofür jeweils ein Gesuch einzureichen ist. Dem Gesuch um Verlängerung sind zudem die bisher gewonnen Resultate beizulegen, was eine vertiefte Prüfung ermöglicht. Hervorzuheben ist schliesslich, dass der Antrag auf Genehmigung eines Auftrags zur Kabelaufklärung praxisgemäss eine Orientierung über den Hintergrund des Auftrags und das nachrichtendienstliche Bedürfnis enthält. Damit werden die verwendeten Suchbegriffe und die gewonnenen Resultate grundsätzlich überprüfbar gemacht. Das Verfahren zur Erteilung der Genehmigung eines Auftrags zur Kabelaufklärung hat jedoch seine inhärenten Grenzen. So lassen sich konkrete Produkte und deren nachrichtendienstlicher Wert nur schwer antizipieren, weshalb die Notwendigkeit eines Auftrags zur Kabelaufklärung zweckmässig erst nach dessen Implementierung anhand konkreter Resultate im Rahmen eines Gesuchs um Verlängerung oder der Kontrolle durch eine unabhängige Behörde beurteilt werden kann. Im Vergleich hierzu wiegt schwerer, dass das anwendbare Recht die Verwendung starker Selektoren keinem Verfahren vorheriger interner beziehungsweise unabhängiger Genehmigung unterwirf. Dieser Mangel wiegt schwer und es wird im Rahmen der Gesamtbeurteilung zu prüfen sein, ob er durch andere Garantien zum Schutz vor Missbrauch aufgewogen oder zumindest gemildert werden kann.

E. 14.5.2

Die Funkaufklärung steht unter keinem Genehmigungsvorbehalt. Dieser Mangel wiegt schwer. Es besteht mithin kein Schutz ex ante gegen missbräuchliche Überwachungsmassnahmen, was in Bezug auf besonders schützenswerte Kommunikationen und die Verwendung von starken Selektoren noch verstärkt ins Gewicht fällt. Ob dieser grundlegende Mangel durch eine effektive Kontrolle durch eine unabhängige Behörde (zumindest) gemindert werden kann, ist im Rahmen der Gesamtbeurteilung zu prüfen. Prüfpunkt 4 Die für die Auswahl, Auswertung und Verwendung des abgefangenen Materials einzuhaltenden Verfahren

E. 15.1

Im Rahmen des vierten Prüfpunktes sind die gesetzlichen Bestimmungen zur Auswahl, Auswertung und Verwendung der erfassten Telekommunikation zu beurteilen (zit. Urteil Centrum för rättvisa, §§ 303 ff.). Hierbei ist zunächst die Rechtsprechung des EGRM im

Zusammenhang mit dem Schutz des Privatlebens (nachfolgend E. 15.2) und der Medienfreiheit (nachfolgend E. 15.3) darzulegen. Anschliessend ist punktuell auf die Rechtsprechung des deutschen Bundesverfassungsgerichts einzugehen (nachfolgend E. 15.4).

E. 15.2

Der Gerichtshof bezeichnet zunächst die Unterscheidung zwischen inländischer und ausländischer Kommunikation und das Verbot, inländische Kommunikation zu überwachen, als eine erhebliche Einschränkung des Ermessens und (damit) als wichtige Garantie zum Schutz vor Missbrauch. Daran ändert nach Ansicht des Gerichtshofs nichts, dass besagte Unterscheidung nicht immer zuverlässig umgesetzt werden kann und auch inländische Kommunikation erfasst wird. Entscheidend ist vielmehr, dass die Beschränkung auf ausländische Kommunikation den Behörden einen verbindlichen Rahmen für ihre Tätigkeit vorgibt. In diesem Sinne verfügen die Genehmigungs-, Überwachungs- und Kontrollbehörden über ein Kriterium für die Beurteilung der Rechtmässigkeit des nachrichtendienstlichen Handelns und damit den Schutz der Rechte des Einzelnen. Das nationale Recht hat daher vorzusehen, dass abgefangene inländische Kommunikation unverzüglich zu löschen ist, sobald sie identifiziert wird. Zudem muss, wie bereits ausgeführt, die Auswahl der Selektoren mit dem Ausschluss der inländischen Kommunikation von der Massenüberwachung im Einklang stehen (zit. Urteil Centrum för rättvisa, §§ 307 f.). Im Weiteren sind nach der Rechtsprechung des EGMR im nationalen Recht die automatische und die manuelle Auswertung der Telekommunikation (anhand von Suchbegriffen), die Aufnahme neuer Suchbegriffe und die Speicherung sowie die Verwendung von Resultaten beziehungsweise Ergebnissen hinreichend bestimmt zu regeln. Dabei ist insbesondere sicherzustellen, dass der manuellen nachrichtendienstlichen Auswertung nur Daten zugänglich sind, die im Rahmen einer genehmigten Massenüberwachung rechtmässig erfasst wurden. Der EGMR prüfte sodann in seinen beiden Entscheidungen Big Brother Watch und andere und Centrum för rättvisa, ob das nationale Recht eine Pflicht zur Protokollierung und detaillierten Aufzeichnung aller Schritte der Massenüberwachung vorsah; jede Datenbearbeitung ist nachvollziehbar und damit überprüfbar zu machen. Das gilt insbesondere für die Verwendung von (neuen beziehungsweise zusätzlichen) Suchbegriffen. Schliesslich ist zu gewährleisten, dass erfasste Daten nur von befugten Personen bearbeitet werden können (zit. Urteile Big Brother Watch und andere, §§ 386 f. und Centrum för rättvisa, §§ 309 ff.).

E. 15.3

Im Zusammenhang mit der Massenüberwachung und dem Schutz von journalistischen Quellen (Art. 10 EMRK) weist der Gerichtshof auf die Gefahr hin, dass im Rahmen einer Überwachung vertrauliches journalistisches Material ohne konkrete Absicht beziehungsweise versehentlich erfasst wird. Die manuelle Analyse der erfassten Telekommunikation durch einen Analysten könne alsdann dazu führen, dass Quellen identifiziert werden. Der EGMR hält es aus diesem Grund für zwingend erforderlich, dass das nationale Recht effektive Schutzvorkehren in Bezug auf die Speicherung, Untersuchung, Verwendung, Weiterleitung und Vernichtung von solch vertraulichem Material vorsieht. Wenn erkannt wird, dass es sich um vertrauliches journalistisches Material handelt, sollte zudem die weitere Bearbeitung und damit die Verwendung der betreffenden Daten nur zulässig sein, wenn ein Gericht oder eine unabhängige Behörde dies zuvor genehmigt hat. Das Gericht oder die Behörde hat dabei insbesondere zu prüfen, ob

die weitere Bearbeitung durch ein überwiegendes öffentliches Interesse gerechtfertigt ist (zit. Urteil Big Brother Watch und andere, §§ 449 f. unter Hinweis insbesondere darauf, dass sich die Umstände mit der zunehmenden Digitalisierung seit dem zit. Urteil Weber und Saravia verändert haben und auch bei einer nicht gezielten und unbeabsichtigten Überwachung eines Journalisten wirksamer Schutz gegen Missbrauch vorzusehen ist).

E. 15.4

Die Aussonderung rein inländischer Kommunikation ist auch im deutschen Recht ein wichtiges Element. Das deutsche Bundesverfassungsgericht weist in diesem Zusammenhang auf das unterschiedliche Eingriffsgewicht hin, das einer Überwachung der ausländischen Kommunikation im Vergleich zur Überwachung der (rein) inländischen Kommunikation zukommt. Es verlangt aus diesem Grund (zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, Rz. 173): [...] Soweit dies [die Aussonderung von (rein) inländischer Kommunikation] technisch möglich ist, muss durch den Einsatz von automatisierten Filterprozessen sichergestellt sein, dass den Mitarbeitern des Bundesnachrichtendienstes solche Telekommunikationsdaten schon gar nicht bekannt werden. Zwar ist es nicht von vornherein unzulässig, wenn, soweit technisch unvermeidbar, zunächst unterschiedslos alle Daten und damit auch die Inlandsdaten von den Systemen des Bundesnachrichtendienstes erfasst werden. Der Gesetzgeber muss dann aber normenklar regeln, dass Daten aus der reinen Inlandskommunikation und gegebenenfalls der Inland-Ausland-Kommunikation mit allen zur Verfügung stehenden Mitteln technisch herausgefiltert und spurenlos gelöscht werden müssen, bevor eine manuelle Auswertung erfolgt. Der Dienst ist darauf zu verpflichten, die Filtermethoden kontinuierlich fortzuentwickeln und auf dem Stand von Wissenschaft und Technik zu halten. Auch im jüngeren Beschluss zur Inland-Ausland-Fernmeldeaufklärung hielt das Bundesverfassungsgericht fest, es bedürfe einer «die Nutzung verfügbarer technischer Möglichkeiten fordernden Regelung zur Aussonderung von Daten aus rein inländischen Telekommunikationsverkehren» (zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Fernmeldeüberwachung, Rz. 165). Es kam sodann sowohl im Urteil zur Ausland-Ausland-Fernmeldeüberwachung als auch im Beschluss zur Inland-Ausland-Fernmeldeüberwachung zum Ergebnis, dass das geltende Recht dieser Anforderung nicht genüge: Es fehle insbesondere an der Pflicht, die Filtermethoden kontinuierlich weiterzuentwickeln. Somit sei nicht hinreichend gewährleistet, dass Daten aus rein inländischer Kommunikation vernichtet würde, bevor eine manuelle Auswertung erfolge (vgl. zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, Rz. 304; zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Fernmeldeaufklärung, Rz. 193).

E. 16.1

Das Nachrichtendienstgesetz unterscheidet bei der Funk- und Kabelaufklärung zwischen der Beschaffung und der nachrichtendienstlichen Auswertung; die Beschaffung von Informationen ist Sache des Beigeladenen (Art. 26 NDV und Art. 2 VEKF), während für die nachrichtendienstliche Auswertung die Vorinstanz zuständig ist (für die Kabelaufklärung ausdrücklich Art. 42 Abs. 5 NDG). Im Folgenden ist zunächst auf die Bestimmungen einzugehen, die für die Auswahl beziehungsweise Beschaffung der erfassten Signale durch den Beigeladenen gelten (nachfolgend E. 16.2.1). Anschliessend ist darzulegen, was das anwendbare Recht in Bezug auf die nachrichtendienstliche Auswertung und Verwendung der Daten durch die Vorinstanz vorschreibt (nachfolgend E. 16.2.2).

E. 16.2.1

Die Vorinstanz kann den Beigeladenen gestützt auf eine Genehmigung des Bundesverwaltungsgerichts und eine Freigabe durch die Vorsteherin oder den Vorsteher des Departements für Verteidigung, Bevölkerungsschutz und Sport VBS damit beauftragen, zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland sowie zur Wahrung weiterer wichtiger Landesinteressen grenzüberschreitende Signale aus leitungsgebundenen Netzen zu erfassen. Der Beigeladene nimmt die Signale der Betreiberinnen und Anbieterinnen nach Art. 41 Abs. 1 Bst. d NDG entgegen, wandelt sie in Daten um und beurteilt anhand des Inhalts, welche Daten er an die Vorinstanz weiterleitet (Art. 42 Abs. 1 NDG). Der Beigeladene nimmt sodann Funkaufklärungsaufträge entgegen und bearbeitet sie (Art. 2 Abs.1 VEKF). Er erfasst und bearbeitet gemäss Art. 2 Abs. 2 VEKF elektromagnetische Ausstrahlungen von Telekommunikationssystemen im Ausland und leitet die Resultate an die Vorinstanz weiter. Im Rahmen eines Auftrags zur Kabelaufklärung leitet der Beigeladene ausschliesslich Daten an die Vorinstanz weiter, die Informationen zu den für die Erfüllung des Auftrags definierten Suchbegriffen enthalten (Art. 39 Abs. 3 NDG und Art. 42 Abs. 2 Satz 1 NDG). Informationen über Personen im Inland leitet der Beigeladene nur dann an die Vorinstanz weiter, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind und zuvor anonymisiert wurden (Art. 42 Abs. 2 Satz 2 NDG). Enthalten die Daten Informationen über Vorgänge im In- oder Ausland, die auf eine konkrete Bedrohung der inneren Sicherheit im Sinne von Art. 6 Abs. 1 Bst. a NDG hinweisen, so leitet der Beigeladene die Daten unverändert an die Vorinstanz weiter (Art. 42 Abs. 3 NDG). Daten, die keine Informationen im Sinne von Art. 42 Abs. 2 und Abs. 3 NDG enthalten, sind vom Beigeladenen so rasch wie möglich zu vernichten (Art. 42 Abs. 4 NDG). Gemäss Art. 28 NDV vernichtet der Beigeladene die im Rahmen der Kabelaufklärung gewonnenen Resultate spätestens im Zeitpunkt der Beendigung des betreffenden Kabelaufklärungsauftrags (Abs. 1). Die erfassten Kommunikationen und die Randdaten sind sodann im Zeitpunkt der Beendigung des Auftrags, spätestens aber 18 Monate (Kommunikationen) beziehungsweise fünf Jahre (Randdaten) nach der Erfassung zu vernichten (Abs. 2 und Abs. 3). Auch im Rahmen der Funkaufklärung werden die erfassten elektromagnetischen Ausstrahlungen durch Anwendung von Suchbegriffen (sog. Targets) durchsucht. Der Beigeladenen leitet sodann nur Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland an die Vorinstanz weiter (Art. 38 Abs. 4 Bst. a NDG); Daten über Personen und Vorgänge im Inland, die als solche erkannt worden sind, hat der Beigeladene grundsätzlich umgehend zu vernichten (vgl. Art. 5 VEKF). Der Beigeladene leitet Informationen über Personen im Inland an die Vorinstanz nur weiter, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind und zuvor anonymisiert wurden (Art. 38 Abs. 4 Bst. b NDG). Wenn jedoch die Informationen auf eine konkrete Bedrohung der inneren Sicherheit im Sinne von Art. 6 Abs. 1 Bst. a NDG hinweisen, leitet der Beigeladene die Informationen unverändert an die Vorinstanz weiter (Art. 38 Abs. 5 NDG). Kommunikationen, die keine Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland beinhalten und keine Hinweise auf eine konkrete Bedrohung der inneren Sicherheit enthalten, vernichtet der Beigeladene gemäss Art. 38 Abs. 6 NDG so rasch wie möglich. Gemäss Art. 4 VEKF vernichtet der Beigeladene die im Rahmen der Funkaufklärung gewonnenen Resultate spätestens im Zeitpunkt der Beendigung des betreffenden Auftrags (Abs. 1). Die erfassten Kommunikationen und die Randdaten sind sodann im Zeitpunkt der Beendigung des Auftrags, spätestens aber 18 Monate (Kommunikationen) beziehungsweise fünf Jahre

(Randdaten) nach deren Erfassung zu vernichten (Abs. 2 und Abs. 3). Der Beigeladene äussert sich insbesondere im Rahmen seiner Antworten zu den Fragenkatalogen des Bundesverwaltungsgerichts zunächst zum Vorgehen, wenn im Rahmen einer Kabelaufklärung eine Kommunikation aufgrund der im Internet üblichen sogenannt paketvermittelten Übertragung nicht vollständig habe erfasst werden können. Entsprechende Daten würden verwendet, wenn Herkunft und (Teil-)Inhalt nachvollziehbar seien und die Auftragsrelevanz gegeben sei (Stellungnahme des Beigeladenen vom 10. November 2022, S. 7). Im Weiteren erläutert der Beigeladene, dass er verschiedene automatische Filter einsetzt, um rein schweizerische Kommunikation und solche mit einem Bezug zur Schweiz (so weit als möglich) markieren zu können. In einem weiteren Schritt würden die gespeicherten Daten durch Anwendung der im Auftrag festgelegten beziehungsweise nachträglich zusätzlich erfassten Selektoren automatisch durchsucht. Schliesslich werde jene Kommunikation, für welche die automatische Suche einen Treffer ergeben habe, von einem Analysten des Beigeladenen analysiert (vgl. ausführlich vorstehend E. 11.2.3). Die Analyse richte sich an der im Auftrag von der Vorinstanz festgelegten Orientierung und am Bedürfnis aus. Im Rahmen der Analyse werde auch überprüft, ob es sich bei (markierten) Kommunikationen um rein schweizerische Kommunikation handle und ob diese Informationen über Personen im Inland enthielten. Handle es sich um eine rein schweizerische Kommunikation, seien die Daten zu vernichten (Art. 39 Abs. 2 NDG). Informationen über Personen im Inland leite der Beigeladene nur weiter, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig und zuvor anonymisiert worden seien (Art. 42 Abs. 2 NDG; vgl. auch Art. 42 Abs. 3 NDG). Die Notwendigkeit erachtet der Beigeladene als gegeben, wenn ein Resultat ohne die Information mit Bezug zum Inland nicht verstanden oder nicht in Kontext gesetzt werden könne oder die Relevanz für die Schweiz nicht ersichtlich sei. Resultate, die anonymisierte Daten über Personen im Inland enthielten, seien nach dem Vieraugenprinzip durch eine vorgesetzte Person im Bereich der Kommunikationsüberwachung (COMINT) freizugeben. Die Anonymisierung werde protokolliert. Eine Anonymisierung könne auf begründeten Antrag der Vorinstanz rückgängig gemacht werden. Über eine solche sogenannte Entanonymisierung entscheide der Leiter des Bereichs Kommunikationsüberwachung (COMINT). Sie werde ebenfalls protokolliert (Stellungnahme des Beigeladenen vom 10. November 2022, S. 10 f.). Es ist davon auszugehen, dass der Beigeladene in Bezug auf das Weiterleiten und Anonymisieren von Informationen über Personen im Inland im Rahmen der Funkaufklärung gleich vorgeht. Schliesslich geht der Beigeladene auf die sogenannte Retrosuche ein. Er legt dar, dass aufgrund der Natur der Kabelaufklärung als ein Mittel der strategischen Aufklärung laufend neue Erkenntnisse gewonnen und (damit) bestehende Erkenntnisse aktualisiert würden. Es sei der Kabelaufklärung daher inhärent, dass bestimmte Signale beziehungsweise Daten erst zu einem späteren Zeitpunkt relevant würden. Auf Anfrage der Vorinstanz würden mithin die Selektoren (erneut) auf die gespeicherten Daten angewendet. Entsprechende Suchen sind gemäss den internen Weisungen, welche der Beigeladene dem Bundesverwaltungsgericht eingereicht hat und die als vertraulich bezeichnet sind, mit Angaben zum Analysten, zu den Suchbegriffen und einem Zeitstempel zu protokollieren (Stellungnahme des Beigeladenen vom 10. November 2022, S. 9 sowie Stellungnahme des Beigeladenen vom 8. März 2024, Beilagen 2 und 3 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Es ist hier mit Blick auf die Bestimmung von Art. 4 Abs. 1-3 VEKF wiederum davon auszugehen, dass der Beigeladene die Retrosuche im dargestellten Rahmen auch bei Daten

aus der Funkaufklärung anwendet.

E. 16.2.2

Die Vorinstanz betreibt zur Erfüllung ihrer Aufgaben gemäss Art. 6 NDG die in Art. 47 Abs. 1 NDG genannten nachrichtendienstlichen Informationssysteme. Das Gesetz legt für jedes Informationssystem in den Grundzügen deren Zweck und Inhalt fest (vgl. Art. 49 ff. NDG) und bildet somit formell-gesetzliche Grundlage für die entsprechende Datenbearbeitung. Hier von Interesse sind im Wesentlichen das Informationssystem zur Geschäftsverwaltung des NDB (GEVER NDB), das der Geschäftsbearbeitung und -kontrolle dient (Art. 52 NDG), das integrale Analysesystem des NDB (IASA NDB), das der nachrichtendienstlichen Auswertung von Daten dient (Art. 49 NDG), und das Informationssystem Kommunikationsaufklärung (ISCO), das der Kontrolle und Steuerung der Funk- und Kabelaufklärung dient (Art. 56 NDG). Das Nachrichtendienstgesetz legt im 4. Kapitel zunächst die Grundsätze der Datenbearbeitung durch die Vorinstanz fest. Gemäss Art. 44 Abs. 1 NDG darf die Vorinstanz Personendaten, einschliesslich besonders schützenswerter Personendaten, bearbeiten. Sie beurteilt sodann die Erheblichkeit und Richtigkeit der Personendaten, bevor sie diese in einem Informationssystem erfasst (Art. 45 Abs. 1 Satz 1 NDG). Meldungen, die mehrere Personendaten enthalten, beurteilt die Vorinstanz als Ganzes, bevor sie diese erfasst (Art. 45 Abs. 1 Satz 2 NDG). Die Vorinstanz erfasst sodann nur Daten, die zur Erfüllung der Aufgaben gemäss Art. 6 NDG dienen. Zudem sind die Datenbearbeitungsschranken gemäss Art. 5 Abs. 5-8 NDG einzuhalten (Art. 45 Abs. 2 NDG). Die Vorinstanz überprüft periodisch in allen Informationssystemen, ob die erfassten Personendaten zur Erfüllung ihrer Aufgaben weiterhin notwendig sind und löscht nicht mehr benötigte Daten. Unrichtige Daten werden korrigiert oder gelöscht (Art. 45 Abs. 4 NDG). Die Vorinstanz kann jedoch Informationen, die sich als Desinformation oder Falschinformation herausstellen, weiter bearbeiten, wenn dies für die Beurteilung der Lage oder einer Quelle notwendig ist. Die betreffenden Daten sind als unrichtig zu kennzeichnen (Art. 44 Abs. 2 NDG). Ferner prüft die interne Qualitätssicherungsstelle in allen Informationssystemen der Vorinstanz stichprobenweise die Rechtmässigkeit, Zweckmässigkeit, Wirksamkeit und Richtigkeit der Datenbearbeitung (Art. 45 Abs. 5 Bst. c NDG). Die Einzelheiten der Datenbearbeitung - die Struktur der Informationssysteme, die Voraussetzungen für eine Datenbearbeitung, die Zugriffsrechte, die Aufbewahrungsdauer etc. - finden sich in der Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB, SR 121.2) geregelt (vgl. Art. 47 Abs. 2 NDG). Gemäss Art. 3 Abs. 1 VIS-NDB prüfen die Mitarbeiterinnen und Mitarbeiter der Vorinstanz vor der Ablage von Originaldokumenten in einem Informationssystem, ob genügend Anhaltspunkte für einen Aufgabenbezug nach Art. 6 NDG gegeben sind (Bst. a), die Datenbearbeitungsschranke nach Art. 5 Abs. 5 NDG eingehalten wird (Bst. b) und die in den Originaldokumenten enthaltenen Informationen aufgrund der Quellenqualität und der Übermittlungsart richtig und erheblich sind (Bst. c). Bestehen Zweifel, so prüfen die das betreffende Originaldokument inhaltlich (Art. 3 Abs. 2 VIS-NDB). In den Erläuterungen zur VIS-NDB ist zu diesen beiden Bestimmungen festgehalten, dass aufgrund der unterschiedlichen Qualität und Menge der Meldungen eine umfassende Prüfung des Inhalts im Sinne von Art. 3 Abs. 1 Bst. c VIS-NDB bei der Ablage oftmals nicht möglich sei; die Überprüfung des Inhalts sei im Gegenteil der Kern der nachrichtendienstlichen Tätigkeit und solle in diesem Rahmen erfolgen. Eine Überprüfung auch des Inhalts müsse jedoch dann in jedem Fall stattfinden, wenn Zweifel an der Richtigkeit bestünden (Art. 3 Abs. 2 VIS-NDB; Erläuterungen zur Verordnung über den Nachrichtendienst

[Nachrichtendienstverordnung, NDV] und zur Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes [VIS-NDB] vom Mai 2022 [nachfolgend: Erläuterungen zu NDV und VIS-NDB] zu Art. 3 VIS-NDB; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 16). Fällt die Prüfung negativ aus, ist das Dokument gemäss Art. 3 Abs. 3 VIS-NDB zu vernichten oder zurückzuschicken. Die Vorinstanz kann sodann die Daten im Rahmen der Ablage mit Hilfe der optischen Zeichenerkennung (OCR-Technik) durchsuchbar machen (Art. 3 Abs. 7 VIS-NDB). Betreffende Dokumente können alsdann mittels Freitextsuche gefunden werden. Weiter ist vor einer personenbezogenen Erfassung von Daten der Aufgabenbezug nach Art. 6 NDG sowie - unter Berücksichtigung der Datenbearbeitungsschranke gemäss Art. 5 Abs. 5 NDG - die Richtigkeit und Erheblichkeit der zu erfassenden Personendaten zu prüfen (Art. 4 Abs. 1 VIS-NDB). Die Vorinstanz äussert sich im Rahmen ihrer Antworten zu den Fragenkatalogen des Bundesverwaltungsgerichts zunächst zu den Selektoren, die auf die gespeicherten Kommunikationen und Randdaten angewendet werden. Demnach werden die Suchbegriffe (im Rahmen der vom Bundesverwaltungsgericht genehmigten Kategorien) zunächst durch die Vorinstanz im Auftrag selbst festgelegt. Stosse der Beigeladene während der beauftragten Suche auf weitere Suchbegriffe, die für den Auftrag relevant sein könnten, könne er selbst Suchbegriffe «vorschlagen bzw. verwenden». Die Vorinstanz erhalte für sämtliche Resultate auch die Suchbegriffe, welche der Beigeladene angewendet habe (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 10 f. [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Die Vorinstanz hält sodann fest, dass Angaben zu einer ausländischen Person als Suchbegriff grundsätzlich zulässig sind. Voraussetzung hierfür sei, dass die betreffende Person im Zusammenhang mit sicherheitspolitisch bedeutsamen Vorgängen im Ausland oder der Wahrung weiterer wichtiger Landesinteressen stehe. Die Kommunikation von Personen im Ausland werde zudem nicht auf allfällige bestehende Berufsgeheimnisse hin überprüft, zumal Informationen über Personen im Ausland auch nicht anonymisiert werden müssten (vgl. Art. 38 Abs. 4 Bst. b und Art. 42 Abs. 2 NDG, jeweils e contrario; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 14). Im Weiteren legt die Vorinstanz dar, Aufträge zur Funk- und Kabelaufklärung würden im Informationssystem Kommunikationsaufklärung (ISCO) erteilt. Auch die Selektoren würden in dieses System aufgenommen und mit dem jeweiligen Aufklärungsauftrag verknüpft. Dasselbe gelte - bei der Kabelaufklärung - für die Genehmigung des Bundesverwaltungsgerichts und die Freigabe durch die Vorsteherin oder den Vorsteher des Departementes für Verteidigung, Bevölkerungsschutz und Sport VBS. Die im Informationssystem Kommunikationsaufklärung (ISCO) erfassten Aufklärungsaufträge und Datenbestände würden sodann jährlich unter Berücksichtigung der aktuellen Lage auf ihre Zweckmässigkeit und Verhältnismässigkeit hin überprüft. Resultate aus der Kabelaufklärung erfasse die Vorinstanz praxisgemäss im integralen Analysesystem (IASA NDB); lasse sich ein Resultat (noch) nicht dem integralen Analysesystem (IASA NDB) zuordnen, etwa, weil der Aufgabenbezug noch nicht in hinreichendem Mass gegeben sei, erfolge eine Ablage im Restdatenspeicher. Die Erfassung beziehungsweise Ablage erfolge als Originaldokument (Art. 2 Bst. d VIS-NDB) zusammen mit einer Bezeichnung des betreffenden Auftrags und mit einem Zeitstempel versehen in den unstrukturierten Daten des integralen Analysesystems (IASA NDB). Eine «nähere Prüfung» im Sinne von Art. 45 Abs. 1 NDG und Art. 3 VIS-NDB finde nicht statt. Die Vorinstanz gehe bei der Ablage von Originaldokumenten mit Blick auf die vorhandenen Ressourcen risikoorientiert vor.

Resultate aus der Funk- und Kabelaufklärung seien bereits vom Beigeladenen analysiert worden, ein Aufgabenbezug sei mithin gegeben. Zudem seien sowohl Funk- als auch Kabelaufklärung Mittel zur Informationsgewinnung im Ausland, weshalb die Datenbearbeitungsschranken (Art. 5 Abs. 5-8 NDG) ohnehin nicht tangiert würden. Die inhaltliche Prüfung der Resultate erfolgt gemäss den Angaben der Vorinstanz «bei der Auswertung und gegebenenfalls bei der Erfassung» der abgelegten Resultate durch Mitarbeitende der Vorinstanz (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 1, S. 7 f.; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 14, 16 f. und 18; vgl. zudem Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 12). Resultate aus der Kabelaufklärung würden zudem auch im Informationssystem zur Geschäftsverwaltung des NDB (GEVER NDB) abgelegt; gemäss der Genehmigungspraxis des Bundesverwaltungsgerichts (Abteilung I, Fachgebiet NDG) seien Resultate einem Gesuch um Verlängerung eines Auftrags zur Kabelaufklärung beizulegen und die betreffenden Gesuche würden im Informationssystem zur Geschäftsverwaltung des NDB (GEVER NDB) bearbeitet (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 1, S. 8). Das Bundesverwaltungsgericht geht davon aus, dass das von der Vorinstanz zur Datenbearbeitung im Zusammenhang mit Resultaten aus der Kabelaufklärung Ausgeführte auch für Resultate aus der Funkaufklärung gilt. Das integrale Analysesystem (IASA NDB) verfügt gemäss den weiteren Angaben der Vorinstanz zusätzlich zur unstrukturierten Fileablage der Originaldokumente über einen strukturierten Teil. In diesem könnten Personen, Sachen oder Ereignisse strukturiert als sogenannte Objekte (Art. 2 Bst. b VIS-NDB) erfasst und die Objekte miteinander verknüpft werden (Art. 2 Bst. h VIS-NDB). Mit dem Objekt würden alsdann alle relevanten Informationen mittels sogenannter Relationen verbunden (Art. 2 Bst. f VID-NDB). Für natürliche und juristische Personen entstehe auf diese Weise ein Personendatensatz (Art. 2 Bst. c VIS-NDB). Das sogenannte Quellendokument schliesslich sei das Ergebnis der strukturierten Erfassung eines Objekts und der damit verbundenen Verknüpfung zu einem oder mehreren Originaldokumenten und weiteren Informationen wie etwa einer Zusammenfassung des Inhalts von Originaldokumenten (Art. 2 Bst. e VIS-NDB); ein Quellendokument sei in diesem Sinne die technische Verbindungsstelle zwischen einem Objekt und einem Originaldokument. Über die strukturierte Erfassung im integralen Analysesystem (IASA NDB) entscheidet gemäss den Angaben der Vorinstanz der zuständige Mitarbeiter aufgrund seines Fachwissens. (Spätestens) im Rahmen der strukturierten Erfassung erfolge sodann auch eine Überprüfung der im Originaldokument enthaltenen Daten auf Richtigkeit und Erheblichkeit sowie auf mögliche Bearbeitungsschranken hin (Art. 4 Abs. 1 VIS-NDB). Objektbezogen erfasst werde jedoch nur ein kleiner Teil der aus der Kabelaufklärung resultierenden Informationen. Die nicht strukturiert erfassten Informationen seien grundsätzlich über die Freitextsuche in den Originaldokumenten zugänglich (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 15 und 18; Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 10; Erläuterungen zu NDV und VIS-NDB zu Art. 3 VIS-NDB). Schliesslich weist die Vorinstanz darauf hin, dass gemäss Art. 45 Abs. 1 Satz 2 NDG Meldungen, die mehrere Personendaten enthalten, als Ganzes beurteilt werden. Nach früherer Auslegung dieser Bestimmung durch die Vorinstanz reichte es aus, wenn die Daten von nur einer der in der Meldung genannten Personen für die Aufgabenerfüllung der Vorinstanz erheblich waren. Eine Anonymisierung der übrigen Personendaten wurde nicht vorgenommen. Diese Praxis sei aufgrund einer Empfehlung der Geschäftsprüfungsdelegation GPDel in deren

Jahresbericht für das Jahr 2019 geändert worden (Stellungnehme der Vorinstanz vom 11. November 2022, Beilage 2, S. 15). Gemäss einer Weisung über die Bearbeitung von Personendaten werden nunmehr Personendaten von Dritten in Originaldokumenten, die in keinem Zusammenhang mit der Aufgabenerfüllung der Vorinstanz stehen, unwiderruflich anonymisiert (Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 13; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 15). Die Vorinstanz weist sodann auf die Möglichkeit der Entanonymisierung hin. Sie führt aus, dass Informationen über Personen im Inland vom Beigeladenen grundsätzlich anonymisiert würden (Art. 38 Abs. 4 Bst. b und Art. 42 Abs. 2 NDG). Ergebe sich jedoch eine konkrete Bedrohung für die innere Sicherheit, dürften die Informationen vom Beigeladenen gemäss Art. 38 Abs. 5 und Art. 42 Abs. 3 NDG unverändert an die Vorinstanz weitergeleitet. Daraus ergebe sich auch die Möglichkeit einer Entanonymisierung: Die nachrichtendienstliche Auswertung von Resultaten aus der Funk- und Kabelaufklärung sei Sache der Vorinstanz. Seien der Vorinstanz Informationen über Personen im Inland anonymisiert weitergeleitet worden und hätten sich im Rahmen der nachrichtendienstlichen Auswertung Hinweise auf eine konkrete Bedrohung der inneren Sicherheit ergeben, müsse die Vorinstanz die Möglichkeit haben, Zugang zu den unveränderten Daten zu erhalten. Hierfür richte sie einen begründeten Antrag auf Entanonymisierung an den Beigeladenen. Zu einem solchen Antrag komme es, wenn der Beigeladene mangels ausreichender Informationen eine konkrete Bedrohung der inneren Sicherheit nicht selbst habe erkennen können. Über die Entanonymisierung entscheidet gemäss der als vertraulich bezeichneten internen Richtlinie für die Entanonymisierung von Informationen aus der Funkaufklärung, die für die Kabelaufklärung analog angewendet wird, der Leiter des Bereichs Kommunikationsüberwachung (COMINT) des Beigeladenen. Jede Entanonymisierung werde protokolliert (Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 7 ff. 22 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 22 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]; zudem die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI, Jahresbericht 2019, im Original zu den Akten genommen mit Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung vom 5. Oktober 2022 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 9. September 2025]). Die Vorinstanz geht im Weiteren auf die Protokollierung beziehungsweise Dokumentation der Bearbeitung von Daten aus der Funk- und Kabelaufklärung ein. Sie verweist hierzu unter anderem auf das als vertraulich bezeichnete Bearbeitungsreglement für das integrale Analysesystem (IASA NDB; Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 13 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Gemäss dem Bearbeitungsreglement muss jede Datenbearbeitung im integralen Analysesystem (IASA NDB) und somit auch das Abrufen und Lesen eines Dokuments zum Zweck des Nachvollzugs im Falle eines Missbrauchs protokolliert werden. Dies gilt nach Angaben der Vorinstanz auch für die Datenbearbeitung im Rahmen der Qualitätskontrolle. Die Protokollierung erfolge automatisiert in Form von Protokolleinträgen in der Datenbank (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 18; Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 13). Die Bearbeitungsreglemente für das Informationssystem zur Geschäftsverwaltung des NDB (GEVER NDB) und für das Informationssystem Kommunikationsaufklärung (ISCO) sehen eine jeweils gleichlautende Pflicht zur Protokollierung der Datenbearbeitung vor (Stellungnahem der Vorinstanz vom

11. November 2022, Beilagen 14 und 20 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Weitere Ausführungen der Vorinstanz betreffen die Qualitätssicherung. Gemäss Art. 20 Abs. 1 VIS-NDB überprüfe einerseits der für die Datenerfassung zuständige Mitarbeiter die Personendatensätze im integralen Analysesystem (IASA NDB) periodisch unter anderem im Hinblick auf die Frage, ob die Bearbeitung notwendig und die Datenbearbeitungsschranken (Art. 5 Abs. 5 und 6 NDG) eingehalten seien. Zusätzlich schreibe Art. 11 Abs. 1 und Abs. 2 VIS-NDB eine Überprüfung im Rahmen von Stichproben durch die Qualitätssicherungsstelle der Vorinstanz vor. Bei strukturiert erfassten Daten beziehe sich die Überprüfung gemäss Art. 11 Abs. 1 VIS-NDB auf den Personendatensatz als Ganzes. Werde im Rahmen der Qualitätssicherung eine unrechtmässige Datenbearbeitung festgestellt, werde das betreffende Dokument entweder gelöscht oder die betreffenden Daten würden anonymisiert (Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 10 f.). Die Pflicht zur periodischen Überprüfung von Personendatensätzen im integralen Analysesystem (IASA NDB) durch die für die Datenerfassung zuständigen Mitarbeitenden ist in einer als vertraulich bezeichneten Weisung weiter konkretisiert (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 16 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Gemäss der Weisung ist jeweils der gesamte Personendatensatz auf seine Relevanz hin zu prüfen. Unrichtige, nicht mehr benötigte oder unter die Datenbearbeitungsschranken fallende Daten sollen korrigiert, gekennzeichnet oder gelöscht werden. Ausschlaggebend für die Berechnung der Fristen gemäss Art. 20 Abs. 3 VIS-NDB sei der Zeitpunkt der Erfassung des ersten Quellendokuments, das mit dem zu überprüfenden Personendatensatz verbunden ist, oder der Zeitpunkt der letzten periodischen Überprüfung. Personendatensätze, deren Überprüfungsfrist (Art. 20 Abs. 3 VIS-NDB) abgelaufen sei, dürften nicht verwendet werden, bevor die periodische Prüfung nachgeholt worden ist. Zusätzlich kontrolliere die Qualitätssicherungsstelle in allen Informationssystemen stichprobenweise die Rechtmässigkeit der Datenbearbeitung und überprüfe quartalsweise, ob Personendatensätze bestehen, deren Überprüfungsfrist abgelaufen ist. Gegebenenfalls beantrage sie bei der Geschäftsleitung Massnahmen. Eine Qualitätssicherung ist auch für die Informationssysteme zur Geschäftsverwaltung des NDB (GEVER NDB) und Kommunikationsaufklärung (ISCO) vorgeschrieben, und zwar sowohl eine solche durch die Mitarbeitenden selbst als auch eine solche durch die Qualitätssicherungsstelle der Vorinstanz (Art. 38 und Art. 59 VIS-NDB). Der Restdatenspeicher sodann wird jährlich stichprobenweise durch die Qualitätssicherungsstelle der Vorinstanz geprüft (Art. 64 VIS-NDB).

E. 16.3.1

Aus der vorstehend dargestellten Rechtsprechung des EGMR ergeben sich die wesentlichen Kriterien, nach denen die für die Auswahl, Auswertung und Verwendung des abgefangenen Materials einzuhaltenden Verfahren zu beurteilen sind: - Unterscheidung zwischen inländischer und ausländischer Kommunikation (nachfolgend E. 16.3.2) - Vorgaben für die Auswertung der Kommunikation (anhand von Suchbegriffen; nachfolgend E. 16.3.3) - Vorhersehbarkeit der Datenbearbeitung (nachfolgend E. 16.3.4) - Protokollierung der Datenbearbeitung (nachfolgend E. 16.3.5) - Schutz vertraulicher Kommunikation (nachfolgend E. 16.3.6)

E. 16.3.2.1

Die Funk- und die Kabelaufklärung dienen der Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland und zur Wahrung wichtiger Landesinteressen (vgl. Art. 38 Abs. 2 NDG; Art. 39 Abs. 1 NDG). Sie setzen hierzu bei der Übertragung grenzüberschreitender Signale über leitungsgebundene Netze beziehungsweise bei der elektromagnetische Ausstrahlung von Telekommunikationssystemen, die sich im Ausland befinden, an. Im Rahmen der Kabelaufklärung darf rein inländische Kommunikation nicht für die nachrichtendienstliche Auswertung durch die Vorinstanz verwendet werden (Art. 39 Abs. 2 Satz 1 NDG; vgl. hierzu vorstehend E. 11.4). Können entsprechende Signale nicht bereits bei der Erfassung ausgeschieden werden, so sind die beschafften Daten zu vernichten, sobald erkannt wird, dass es sich um rein inländische Kommunikation handelt (Art. 39 Abs. 2 Satz 2 NDG). Darüber hinaus leitet der Beigeladene Informationen über Personen im Inland grundsätzlich nur dann an die Vorinstanz weiter, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind und zuvor anonymisiert wurden (Art. 38 Abs. 4 Bst. b und Art. 42 Abs. 2 NDG). Das Verbot der Verwendung rein inländischer Kommunikation im Rahmen der Kabelaufklärung und die Einschränkungen in Bezug auf die Bekanntgabe von Informationen über Personen im Inland schränken das Ermessen der Behörden, wie im Rahmen des Prüfpunktes 2 bereits ausgeführt, in erheblichem Mass sowie in vorhersehbarer Weise ein und bieten insoweit grundsätzlich Schutz vor Missbrauch (vgl. zit. Urteil Centrum för rättvisa, § 308). Für die Funkaufklärung schreibt das Gesetz kein Verbot der Verwendung rein inländischer Kommunikation vor und es liegen dem Bundesverwaltungsgericht keine Angaben darüber vor, ob in der Praxis ein entsprechendes Verwendungsverbot gilt. Mit Blick auf die Pflicht, Informationen über Personen im Inland grundsätzlich zu anonymisieren, fällt dieser Mangel jedoch nicht erheblich ins Gewicht (vgl. auch vorstehend E. 12.2).

E. 16.3.2.2

Von der Verwendung im Rahmen der Kabelaufklärung ist nur rein schweizerische Kommunikation ausgeschlossen (Art. 39 Abs. 2 NDG). Befindet sich der Empfänger oder der Sender einer Kommunikation im Ausland, darf die erfasste Kommunikation verwendet werden. Informationen über Personen im Inland leitet der Beigeladene jedoch nur dann an die Vorinstanz weiter, wenn sie für das Verständnis eines Vorgangs im Ausland notwendig sind und zuvor anonymisiert wurden. Letzteres ist auch für die Funkaufklärung vorgeschrieben. Die Pflicht zur Anonymisierung gilt dabei nicht in jedem Fall. Enthalten die Daten Informationen über Vorgänge im In- und Ausland, die auf eine konkrete Bedrohung der inneren Sicherheit hinweisen, so leitet der Beigeladene die Daten unverändert an die Vorinstanz weiter (Art. 38 Abs. 5 und Art. 42 Abs. 3 NDG). Zusätzlich besteht die Möglichkeit der nachträglichen Entanonymisierung (vgl. hierzu auch vorstehend E. 16.2.2 und [zur Vorhersehbarkeit der Datenbearbeitung] nachfolgend E. 16.3.4.3). Das Gesetz erlaubt mithin unter bestimmten Voraussetzungen die Verwendung von Daten über Personen im Inland, die im Zusammenhang mit der Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland anfallen, was jedoch am Charakter der Funk- und Kabelaufklärung grundsätzlich nichts ändert (vgl. auch vorstehend E. 9.4 betreffend Informationsbeschaffungen mit einem Inland-Bezug). Die Schutzwirkung, die sich aus der Unterscheidung von inländischer und ausländischer Kommunikation verbunden mit dem Verbot der Verwendung rein inländischer Kommunikation und aus der Pflicht zur Anonymisierung ergibt, wird jedoch gleichwohl vermindert. Die Pflicht, Informationen über Personen im Inland unter Umständen unverändert an die Vorinstanz weiterzuleiten, birgt mithin ein nicht unerhebliches Missbrauchspotential, insbesondere,

wenn Aufträge zur Funk- und Kabelaufklärung einen Schweiz-Bezug aufweisen; die Funk- und Kabelaufklärung könnten zur Beschaffung von Informationen über Personen im Inland missbraucht werden. Dabei ist mitentscheidend, dass die Weiterleitung beziehungsweise nachträgliche Entanonymisierung nicht unter einem Genehmigungsvorbehalt durch eine unabhängige Behörde steht. Bei der Wahrung der inneren Sicherheit handelt es sich jedoch um ein zulässiges öffentliches Interesse im Sinne von Art. 8 Ziff. 2 EMRK und weder die Funk- noch die Kabelaufklärung dürfen auf die Beschaffung von Informationen über Vorgänge im Inland ausgerichtet sein. Es ist daher nicht von vornherein ausgeschlossen, dass dieser Mangel durch eifne effektive Überwachung kompensiert wird. Dies wird im Rahmen der Gesamtbeurteilung unter Berücksichtigung der Ergebnisse zu Prüfpunkt 7 zu prüfen sein. Zu beachten ist in diesem Zusammenhang auch die Bestimmung im Nachrichtendienstgesetz zur Bekanntgabe von Personendaten an inländische Behörden. Dienen Erkenntnisse, welche die Vorinstanz etwa im Zusammenhang mit der Funk- und Kabelaufklärung gewonnen hat, anderen Behörden unter anderem zur Strafverfolgung, so stellt die Vorinstanz ihnen diese unaufgefordert oder auf Anfrage hin zur Verfügung (Art. 60 Abs. 2 NDG). Besondere Anforderungen beziehungsweise Hürden, wie sie etwa Art. 60 Abs. 3 NDG für die Bekanntgabe von Erkenntnissen aus genehmigungspflichtigen Beschaffungsmassnahmen im Sinne von Art. 26 ff. NDG vorsieht, bestehen nicht (vgl. zu den Anforderungen an eine Bekanntgabe im deutschen Recht § 7 Abs. 5 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel 10-Gesetz; G 10], und § 11 des Gesetzes über den Bundesnachrichtendienst [BND-Gesetz; BNDG], beide abrufbar unter < www.gesetze-im-internet.de > Gesetze/Verordnungen > G 10 bzw. BNDG). Es reicht vielmehr aus, dass Erkenntnisse den Behörden zur Strafverfolgung «dienen» (vgl. hierzu bereits vorstehend E. 6.3.4). Aus Sicht des Datenschutzrechts stellt die Bekanntgabe eine Zweckänderung dar, die im Gesetz vorgesehen und die verhältnismässig sein muss. Zudem ist hier die Gefahr zu beachten, dass die Kabelaufklärung als ein Mittel der präventiven nachrichtendienstlichen Tätigkeit für repressive Zwecke «missbraucht» wird: So ist von der Verwendung im Rahmen der Kabelaufklärung nur die rein inländische Kommunikation ausgeschlossen; befindet sich nur entweder der Sender oder der Empfänger in der Schweiz, darf die erfasste Kommunikation verwendet werden. Die erfassten Kommunikationen (einschliesslich der Randdaten) werden zudem über einen langen Zeitraum aufbewahrt, so dass die Selektoren - auch neue beziehungsweise zusätzliche Selektoren - erneut angewandt werden können. Auch vor diesem Hintergrund ist mit der Möglichkeit der Bekanntgabe von Informationen über Personen im Inland in nicht anonymisierter Form beziehungsweise mit er Möglichkeit der Entanonymisierung ein Missbrauchspotential verbunden; wie bereits das Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) ausgeführt hat, können diese Möglichkeiten zur Folge haben, dass Personen im Inland zum Ziel weiterer Massnahmen der Schweizerischen Behörden werden. Zwar ist eine solche Bekanntgabe beziehungsweise Entanonymisierung nur möglich, wenn Hinweise auf eine konkrete Bedrohung der inneren Sicherheit bestehen, was die Möglichkeiten einer Entanonymisierung einschränkt. Gleichwohl kann unter Berücksichtigung der gesamten Umstände nicht gesagt werden, ein «Missbrauch» der Kabelaufklärung zum Zweck etwa der Strafverfolgung sei theoretisch nur sehr entfernt möglich. Dabei fällt besonders ins Gewicht, dass das anwendbare Recht eine Bekanntgabe von Erkenntnissen aus der Kabelaufklärung an die Strafverfolgungsbehörden - und damit verbunden aus datenschutzrechtlicher Sicht eine Zweckänderung - im Wesentlichen voraussetzungslos zulässt. Vorausgesetzt ist lediglich, dass die Erkenntnisse der

Strafverfolgung dienen. Das Gesetz verlangt mithin keine Abwägung der widerstreitenden Interessen. Eine solche Interessenabwägung wäre zudem verfahrensrechtlich abzusichern, indem eine Bekanntgabe erst nach erfolgter Genehmigung durch eine unabhängige Behörde erfolgen dürfte (vgl. in diesem Zusammenhang das zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, Rz. 174). Die Bekanntgabe wird, soweit ersichtlich, auch nicht protokolliert. Das Gesetz enthält somit auch in Bezug auf die Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an Behörden etwa zur Strafverfolgung keine ausreichenden Garantien zum Schutz vor Missbrauch und erweist sich insofern als mangelhaft.

E. 16.3.2.3

Das anwendbare Recht verlangt sodann nicht, dass im Rahmen der Kabelaufklärung die Methoden zur Aussonderung von rein schweizerischer Kommunikation kontinuierlich weiterzuentwickeln sind. Das Gesetz ist in dieser Hinsicht final formuliert; es wird verlangt, dass rein schweizerische Kommunikation auszusondern ist, eine bestimmte (technische) Methode etwa zur Filterung von erfassten Kommunikationen ist jedoch nicht vorgeschrieben. Angesichts der technischen Entwicklung, die auch den EGMR zu einer Weiterentwicklung seiner Rechtsprechung veranlasst hat (vgl. vorstehend E. 7.3), reicht die final angeleitete Pflicht zur Aussonderung rein schweizerischer Kommunikation nicht aus. Das Gesetz muss vielmehr verpflichtend vorschreiben, die Kabelaufklärung insbesondere hinsichtlich der Aussonderung rein inländischer Kommunikation (technisch) kontinuierlich weiterzuentwickeln. Immerhin ergibt sich aus der Praxis, dass der Beigeladene in dieser Hinsicht nicht untätig ist; den Berichten der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI kann entnommen werden, dass der Beigeladene die Erfassung rein schweizerischer Kommunikation durch eine kontinuierliche Weiterentwicklung seiner Tätigkeit und insbesondere der technischen Infrastruktur zu vermeiden sucht. Der Mangel in Bezug auf die gesetzliche Regelung kann damit immerhin gemindert, nicht aber beseitigt werden.

E. 16.3.3

In einem nächsten Schritt ist auf die Vorgaben in Bezug auf die Auswertung der gespeicherten Kommunikationen (anhand von Suchbegriffen) einzugehen. Das anwendbare Recht sieht eine organisatorische Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung vor. Aufträge zur Funk- und Kabelaufklärung werden von der Vorinstanz erteilt. Die Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland ist sodann Aufgabe des Beigeladenen. Dieser erfasst grenzüberschreitende Signale aus leitungsgebundenen Netzten, wandelt die Signale um und durchsucht die gewonnenen Daten durch Anwendung spezifischer Selektoren. In einem weiteren Schritt wertet er die Treffer manuell aus. Hierbei dienen die Aufträge - insbesondere die Angaben zu Orientierung und zum Bedürfnis (vgl. hierzu vorstehend E. 14.2.1) - als verbindlicher Rahmen. Der Beigeladene leitet sodann ausschliesslich Daten an die Vorinstanz weiter, die Informationen zu den für die Erfüllung des Auftrags definierten Suchbegriffen enthalten (Art. 42 Abs. 2 NDG). Die Vorinstanz wertet die weitergeleiteten Daten anschliessend aus und speichert sie insbesondere im integralen Analysesystem (IASA NDB; vgl. zur Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung bereits vorstehend E. 11.4.3). Die Vorinstanz hat keinen unmittelbaren Zugriff auf die vom Beigeladenen erfassten Signale und der Beigeladene wiederum hat keinen Zugriff auf das integrale Analysesystem (IASA NDB) der Vorinstanz. Die dargestellte

organisatorische Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung von beschafften Daten stellt eine wichtige Garantie zum Schutz vor Missbrauch dar (vgl. auch Isenring/Quiblier, a.a.O., S. 138 in fine). Die Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung wird in der Praxis nicht konsequent umgesetzt. Gemäss Art. 27 Abs. 4 NDV und Art. 2 Abs. 5 VEKF kann der Beigeladene der Vorinstanz vorschlagen, im Rahmen der (genehmigten und freigegebenen) Aufträge zusätzliche Suchbegriffe in laufende Aufträge aufzunehmen. Den Angaben der Vorinstanz zufolge entscheidet der Beigeladene darüber in der Praxis weitgehend eigenständig; eine vorgängige Zustimmung der Vorinstanz ist nicht erforderlich. Vielmehr weist der Beigeladene zusammen mit Resultaten, die er der Vorinstanz weiterleitet, zusätzliche Suchbegriffe aus (vgl. vorstehend E. 16.2.2). Es erscheint fraglich, ob diese Praxis mit der Bestimmung von Art. 27 Abs. 4 NDV und Art. 2 Abs. 5 VEKF konform ist, die nach ihrem Wortlaut einen Genehmigungsvorbehalt zu Gunsten der Vorinstanz statuieren; ein solcher Vorbehalt ergibt sich auch bei einer systematischen und teleologischen Betrachtungsweise, wonach die Vorinstanz durch den Auftrag zur Aufklärung deren Rahmen festlegt und der Beigeladene im Wesentlichen ausführend für die Informationsbeschaffung zuständig ist (vgl. hierzu auch die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI, Jahresbericht 2021 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 9. September 2025], wonach der Gesetzgeber von einer weniger weitgehenden Mitwirkung des Beigeladenen ausgegangen ist). Die Garantie zum Schutz vor Missbrauch, die sich aus der Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung ergibt, wird durch die Praxis, wonach der Beigeladene weitgehend selbständig neue Suchbegriffe in einen laufenden Auftrag aufnehmen kann, jedoch nicht entscheidend geschmälert.

E. 16.3.4.1

Die Umstände, unter denen die Kommunikation eines Individuums überwacht werden darf, sind gemäss den vorstehenden Ausführungen ausreichend vorhersehbar (vgl. vorstehend E. 10-12). Das gilt im Grundsatz auch für die weitere Datenbearbeitung durch den Beigeladenen (Filtern, Anwendung von Selektoren, manuelle Analyse soweit das Weiterleiten von Daten an die Vorinstanz) und die Vorinstanz (Ablage in einem Informationssystem, nachrichtendienstliche Auswertung und Verwendung der Daten sowie die Qualitätskontrolle). Die Berechtigung für den Zugriff auf Daten beziehungsweise Informationssysteme erfolgt zudem sowohl beim Beigeladenen als auch bei der Vorinstanz rollenbezogen und ist insofern eingeschränkt. Auf einzelne Aspekte der Anwendungspraxis ist jedoch im Folgenden näher einzugehen.

E. 16.3.4.2

Die Vorinstanz legt Resultate aus der Kabelaufklärung nach eigenen Angaben unverändert im integralen Analysesystem (IASA NDB) ab; die Originaldokumente werden insbesondere nicht auf ihre Richtigkeit und Erheblichkeit sowie auf Einhaltung der Datenbearbeitungsschranke (Art. 5 Abs. 5-8 NDG) geprüft. Mangels Angaben zu einer abweichenden Praxis im Rahmen der Funkaufklärung ist davon auszugehen, dass auch Resultate aus der Funkaufklärung bei ihrer Erfassung nicht auf ihre Richtigkeit und Erheblichkeit sowie auf Einhaltung der Datenbearbeitungsschranke geprüft werden. Die Vorinstanz hält hierzu fest, Resultate aus der Kabelaufklärung seien bereits durch einen Analysten des Beigeladenen auf ihre Erheblichkeit hin überprüft worden und zudem sei die Datenbearbeitungsschranke im Rahmen der Auslandsaufklärung nicht von Bedeutung (vgl.

vorstehend E. 16.2.2). Zu dieser Praxis ist zunächst festzuhalten, dass sie Gesetz (Art. 45 Abs. 1 NDG) und Verordnung (Art. 3 Abs. 1 VIS-NDB) widerspricht. Sie steht zudem im Widerspruch zu der vom Gesetzgeber gewollten Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung. Für die nachrichtendienstliche Auswertung ist die Vorinstanz zuständig. Ihr obliegt es mithin auch, die Richtigkeit und Erheblichkeit von Originaldokumenten zu prüfen. Zudem erfolgt die Analyse, die der Beigeladene vornimmt, auftragsbezogen. Sie vermag daher eine aufgabenbezogene Beurteilung, wie sie Art. 45 Abs. 1 NDG und Art. 3 Abs. 1 VIS-NDB vorschreibt, nicht zu ersetzen. Die Vorinstanz gibt sodann an, die Prüfung, ob die im Originaldokument enthaltenen Informationen richtig und erheblich sind, und ob die Bearbeitungsschranke eingehalten werden, erfolge im Rahmen der Auswertung der Resultate aus der Kabelaufklärung. Die Pflicht, eine solche Prüfung im Rahmen der Auswertung vorzunehmen, ergibt sich jedoch weder aus dem Gesetz noch (unmittelbar) aus der Weisung über die Handhabung von Personendaten durch die Vorinstanz, auf welche sie verweist (Stellungahme der Vorinstanz vom 11. November 2022, Beilage 15). Vielmehr verweist das Datenschutzkonzept der Vorinstanz auf besagten Art. 3 Abs. 1 VIS-NDB und schreibt insoweit eine Prüfung bei der Ablage von Informationen vor (Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 10 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025]). Der Vorinstanz steht zudem in ihren Informationssystemen eine Freitextsuche zur Verfügung. Damit sind Originaldokumente auffindbar, auch wenn sie nicht strukturiert erfasst worden sind. Diese Dokumente müssten vor einer weiteren Verwendung zunächst auf ihre Richtigkeit und Erheblichkeit sowie auf Einhaltung der Datenbearbeitungsschranke gemäss Art. 5 Abs. 5 NDG geprüft werden. Damit eine solche Prüfung im Rahmen der weiteren Verwendung erfolgen kann, wären die betreffenden Daten zuvor (automatisch) zumindest zu kennzeichnen. Ob eine entsprechende Pflicht beziehungsweise Praxis besteht, ergibt sich aus den Darlegungen der Vorinstanz nicht. Und selbst wenn eine solche Kennzeichnung intern vorgeschrieben oder Praxis wäre, bestünde ein nicht unerhebliches Missbrauchspotential, da eine Verwendung auch ohne eine solche Prüfung möglich wäre. Eine hinreichende Gewähr dafür, dass Daten auf ihre Erheblichkeit und Richtigkeit geprüft werden, besteht somit nur, wenn besagte Prüfung vor beziehungsweise bei der Erfassung der Originaldokumente erfolgt. Schliesslich ist die Prüfung bei der Ablage von Resultaten auch aus einem weiteren Grund von Bedeutung: Wird bei beziehungsweise vor der Ablage festgestellt, dass Daten etwa aufgrund eines fehlenden Aufgabenbezugs unrechtmässig bearbeitet werden, werden sie vernichtet oder anonymisiert. Wird hingegen die Unrechtmässigkeit der Datenbearbeitung zu einem späteren Zeitpunkt festgestellt, werden die Daten gelöscht und dem Schweizerischen Bundesarchiv BAR zur Übernahme angeboten (vgl. hierzu ausführlich nachfolgend E. 18.2.2). Eine Vernichtung der Daten ist damit - soweit aufgrund der Angaben der Vorinstanz zu ihrer Praxis ersichtlich - nur gewährleistet, wenn die Prüfung auf Erheblichkeit und Richtigkeit bei der Ablage erfolgt. Insgesamt besteht daher ein gewichtiges Interesse daran, dass die Vorinstanz nur Daten bearbeitet, deren Erheblichkeit und Richtigkeit sie vorab geprüft hat (vgl. in diesem Sinne auch Art. 45 Abs. 1 NDG). Im Ergebnis ist daher festzuhalten, dass die Anwendungspraxis der Vorinstanz keine hinreichende Gewähr dafür bietet, dass nur richtige und erhebliche Daten bearbeitet werden (vgl. zur Kennzeichnungspflicht unrichtiger Informationen Art. 44 Abs. 2 NDG, was wiederum eine vorgängige Prüfung voraussetzt). Ob dieser Mangel durch andere Garantien ausgeglichen werden kann, wird im Rahmen der Gesamtbeurteilung zu prüfen sein. Mit der laufenden Revision des Nachrichtendienstgesetzes soll die

Datenhaltung der Vorinstanz vollständig neu geregelt werden. Neu würde zwischen nachrichtendienstlichen und administrativen Daten unterschieden. Für die nachrichtendienstlichen Daten sind sodann verschiedene Unterkategorien vorgesehen, die grundsätzlich den heutigen Informations- und Speichersystemen entsprechen. Zum Zeitpunkt des Eingangs der Daten würde zunächst geprüft, ob es sich um nachrichtendienstliche oder administrative Daten handelt; die Daten würden entsprechend gekennzeichnet. Nachrichtendienstliche Daten sollen zudem daraufhin überprüft werden, ob ein hinreichender Aufgabenbezug gegeben und eine Datenbearbeitungsschranke gemäss Art. 5 Abs. 5-8 NDG tangiert ist (Eingangsprüfung). Besteht ein hinreichender Aufgabenbezug und sind die Datenbearbeitungsschranken eingehalten, würden die Daten als sogenannte Rohdaten erfasst. Rohdaten dürften erst weiterbearbeitet werden, wenn die Richtigkeit und Relevanz der Daten überprüft worden ist. Die betreffenden Daten wären hiernach zudem als sogenannte Arbeitsdaten zu kennzeichnen. Dabei wäre für Daten aus genehmigungspflichtigen Beschaffungsmassnahmen keine umfassende Eingangsprüfung erforderlich; die Einhaltung der Datenbearbeitungsschranken würde ebenso wie die Erheblichkeit und Richtigkeit der Daten erst dann geprüft, wenn die Daten für eine vertiefte Weiterbearbeitung als Arbeitsdaten gekennzeichnet werden sollen (Erläuternder Bericht Revision NDG zum 4. Kapitel: Datenbearbeitung und Qualitätssicherung). Ob dies auch für Ergebnisse aus der Funk- und Kabelaufklärung gilt, ergibt sich aus dem Entwurf, der in die Vernehmlassung gegeben worden ist, nicht. Ebenso bleibt offen, ob mittels der Freitextsuche auch in Rohdaten gesucht werden kann - so, wie bisher auch in Originaldokumenten gesucht werden konnte. Damit bestünde - soweit ersichtlich - weiterhin keine hinreichende Gewähr dafür, dass die Vorinstanz nur richtige und erhebliche Daten bearbeitet. Die Vorinstanz speichert die Resultate aus der Funk- und Kabelaufklärung praxisgemäss zur nachrichtendienstlichen Verwendung im integralen Analysesystem (IASA NDB) oder im Restdatenspeicher. Zusätzlich werden die Resultate zur Steuerung der Funk- und Kabelaufklärung im Informationssystem Kommunikationsaufklärung (ISCO) und im Hinblick auf eine allfällige Verlängerung eines Auftrags zur Kabelaufklärung im Informationssysteme zur Geschäftsverwaltung des NDB (GEVER NDB) gespeichert. Der Umstand, dass Resultate aus der Funk- und Kabelaufklärung in verschiedenen Informationssystemen bearbeitet werden, erhöht das Risiko von Missbrauch, da unterschiedliche Personen in unterschiedlichen Funktionen beziehungsweise mit unterschiedlichen Rollen Zugang zu Resultaten aus der Funk- und Kabelaufklärung haben. Der Umstand, dass Resultate in verschiedenen Informationssystemen bearbeitet werden, ist jedoch gleichzeitig Folge einer zum Schutz vor Missbrauch geschaffenen differenzierten Architektur zur Datenbearbeitung; die Mitarbeitenden sollen Zugriff nur auf jene Daten haben, die sie zur Erfüllung ihrer Aufgaben benötigen. Das Risiko, das mit einer Bearbeitung von Resultaten aus der Funk- und Kabelaufklärung in verschiedenen Informationssystemen geschaffen wird, ist daher hinzunehmen.

E. 16.3.4.3

Weiter besteht nach den Ausführungen der Vorinstanz die Möglichkeit einer sogenannten Entanonymisierung. Gemäss Art. 38 Abs. 4 Bst. b NDG und Art. 42 Abs. 2 NDG leitet der Beigeladene Informationen über Personen im Inland grundsätzlich anonymisiert an die Vorinstanz weiter. Enthalten die Daten jedoch Informationen über Vorgänge im In- oder Ausland, die auf eine konkrete Bedrohung für die innere Sicherheit hinweisen, werden die Daten nicht anonymisiert (Art. 38 Abs. 5 und Art. 42 Abs. 3 NDG). Gemäss den Angaben

der Vorinstanz vermag der Beigeladene derartige Bedrohungssituationen in der Praxis nicht immer zu erkennen. Die Vorinstanz begründet dies damit, dass dem Beigeladenen, der nicht für die nachrichtendienstliche Auswertung zuständig ist, hierfür nicht die erforderlichen Informationen zur Verfügung stünden. Aus diesem Grund stelle die Vorinstanz jeweils einen Antrag auf Entanonymisierung, wenn sich aus den Daten Hinweise auf eine konkrete Bedrohung der inneren Sicherheit ergeben, die Daten jedoch vom Beigeladenen zuvor anonymisiert wurden (vgl. hierzu vorstehend E. 16.2.2). Das Interesse, das hinter dieser Anwendungspraxis steht, ist sachlich begründet und deckt sich mit der Zweckrichtung von Art. 38 Abs. 5 und Art. 42 Abs. 3 NDG (vgl. bereits vorstehend E. 16.3.2.2 und das zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Aufklärung, Rz. 278, wonach die ausnahmsweise Verwendung von Informationen über Personen im Inland weitergehend als gemäss dem hier anwendbaren Recht einer «gerichtsähnlichen» Kontrolle bedarf). Es fragt sich jedoch, ob die Möglichkeit der nachträglichen Entanonymisierung auf der Grundlage des geltenden Rechts hinreichend vorhersehbar ist. Die Frage kann hier offen bleiben. Gestützt auf Art. 38 Abs. 5 und Art. 42 Abs. 3 NDG ist in hinreichendem Mass vorhersehbar, dass Informationen über Personen im Inland nicht in jedem Fall anonymisiert werden, sondern im Falle von Hinweisen auf eine Gefährdung der inneren Sicherheit unverändert an die Vorinstanz weitergeleitet werden. Ob die Daten von vornherein unverändert übermittelt werden oder die Vorinstanz im Nachgang ein Gesuch um Entanonymisierung stellt, ist daher letztlich nicht entscheidend (vgl. Art. 5 Abs. 1 VEKF, der zur Möglichkeit der nachträglichen Anonymisierung in einem gewissen Widerspruch steht).

E. 16.3.4.4

Nach Angaben des Beigeladenen und der Vorinstanz besteht in der Anwendungspraxis sodann die Möglichkeit einer sogenannten Retrosuche. Hierbei wendet der Beigeladene die Selektoren - auch zwischenzeitlich zusätzlich beziehungsweise neu definierte Selektoren - (erneut) auf die gespeicherten Daten an. Er bewahrt hierzu die erfassten Kommunikationen bis zu 18 Monate und die erfassten Randdaten bis zu fünf Jahre auf (Art. 28 Abs. 2 und 3 NDV, Art. 4 Abs. 2 und 3 VEKF; vgl. hierzu vorstehend E. 16.2.1). Die Möglichkeit einer Retrosuche ergibt sich nicht unmittelbar aus dem anwendbaren Recht. Vielmehr schreiben Art. 38 Abs. 6 und Art. 42 Abs. 4 NDG vor, dass Daten, die keine Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland beziehungsweise keine Hinweise auf eine konkrete Bedrohung der inneren Sicherheit enthalten, «so rasch als möglich» zu vernichten sind (vgl. auch BGE 151 I 137 E. 3.6.3). Die Möglichkeit, die erfassten Kommunikationen und die Randdaten bis zur Beendigung des Auftrags, längstens aber 18 Monate beziehungsweise fünf Jahre aufzubewahren, kann daher nicht als von vornherein konform mit Art. 38 Abs. 6 und Art. 42 Abs. 4 NDG bezeichnet werden (vgl. auch Art. 38 Abs. 3 und Art. 39 Abs. 4 Bst. c NDG, wonach der Bundesrat die maximale Aufbewahrungsdauer der erfassten Daten regelt). Immerhin ergibt sich aus der Möglichkeit (aber nicht ohne Weiteres die Erlaubnis), die erfasste Kommunikation und die Verbindungsdaten über einen längeren Zeitraum aufzubewahren, implizit die Möglichkeit, die betreffenden Daten auch zu einem späteren Zeitpunkt (erneut) zu verwenden. Die Möglichkeit einer Retrosuche ist denn auch in den Erläuterungen zur Nachrichtendienstverordnung erwähnt (vgl. Erläuterungen zu NDV und VIS-NDB zu Art. 28 NDV). Insgesamt bleibt jedoch fraglich, ob die Möglichkeit einer Retrosuche und damit eine weitere Datenbearbeitung gestützt auf das geltende Recht für die Beschwerdeführenden hinreichend vorhersehbar ist. Ins Gewicht fallen dabei auch die

langen Aufbewahrungsfristen, womit eine erneute Datenbearbeitung auch nach Jahren noch möglich ist. Es ist jedoch nicht von vornherein ausgeschlossen, dass der Mangel an Vorhersehbarkeit durch eine laufende Überwachung der nachrichtendienstlichen Tätigkeit kompensiert wird. Dies wird im Rahmen der Gesamtbeurteilung unter Berücksichtigung der Ergebnisse zu Prüfpunkt 7 zu prüfen sein.

E. 16.3.5

Nach der Rechtsprechung des EGMR stellt die Pflicht zur Protokollierung und Aufzeichnung aller Schritte einer Massenüberwachung eine wichtige Garantie zum Schutz vor Missbrauch dar (vgl. vorstehend E. 7.3.3 und E. 15.2). Für die Funk- und Kabelaufklärung ist eine entsprechende Pflicht jedoch nur in internen Weisungen - den Bearbeitungsreglementen für die verschiedenen Informationssysteme - enthalten. Diese sind zudem nicht öffentlich zugänglich. Das anwendbare Recht bietet insoweit keinen hinreichenden Schutz gegen Missbrauch. Es besteht jedoch kein Grund zu der Annahme, dass die Weisungen nicht angewendet oder die Pflicht zur Protokollierung abgeändert würden. Die Protokollierungspflicht ist zudem umfassend; jede Datenbearbeitung einschliesslich Angaben zu Urzeit und Name des Mitarbeiters wird automatisch festgehalten. Der Mangel kann daher durch eine hinreichende Kontrolle durch eine unabhängige Behörde ausgeglichen werden (vgl. in diesem Sinne auch das zit. Urteil Centrum för rättvisa, § 311). Ob dies der Fall ist, wird im Rahmen der abschliessenden Gesamtbeurteilung zu prüfen sein (vgl. nachfolgend E. 25).

E. 16.3.6.1

Im Besonderen einzugehen ist im Folgenden auf Kommunikationsbeziehungen, denen besonderer Schutz zukommt. Das betrifft etwa die Kommunikationsbeziehung zwischen einem Journalisten und seiner Quelle oder zwischen einem Rechtsanwalt und seinem Mandanten.

E. 16.3.6.2

Der EGMR verlangt im Zusammenhang mit der Beeinträchtigung von Art. 10 EMRK, dass das nationale Recht auch und gerade im Rahmen einer Massenüberwachung effektive Schutzvorkehren in Bezug auf die Speicherung, Untersuchung, Verwendung, Weiterleitung und Vernichtung von vertraulichem journalistischem Material enthält; erforderlich ist eine ausreichende verfahrensrechtliche Sicherung der konventionsrechtlichen Garantie (vgl. vorstehend E. 15.3). Das für die Funk- und Kabelaufklärung anwendbare Recht enthält keine Schutzvorkehren in Bezug auf den journalistischen Quellenschutz. Zwar sieht Art. 58 Abs. 3 NDG in Bezug auf unter anderem den Quellenschutz von Medienschaffenden vor, dass entsprechende Daten unter der Leitung des Bundesverwaltungsgerichts ausgesondert werden (vgl. auch Art. 23 NDV). Diese Schutzvorkehrung gilt jedoch nur für die sogenannt genehmigungspflichtigen Beschaffungsmassnahmen (vgl. hierzu vorstehend E. 6.3.4). Die Vorinstanz führt in diesem Zusammenhang aus, Angaben über schweizerische natürliche und juristische Personen seien als Suchbegriffe nicht zulässig (vgl. Art. 39 Abs. 3 NDG) und Informationen über Personen im Inland würden, wenn diese weitergeleitet würden, zuvor grundsätzlich anonymisiert (vgl. Art. 42 Abs. 2 NDG). Zudem werde besonders geschützte Kommunikation vom Beigeladenen ausgesondert, sofern sie sich erkennen lasse (Stellungnahme der Vorinstanz vom 12. April 2024, S. 9). Damit bestünden hinreichende Garantien zum Schutz vor Missbrauch. In den persönlichen Schutzbereich von Art. 10 EMRK fallen nach der Rechtsprechung des EGMR nicht nur Personen im Inland. Vielmehr

können sich auch journalistisch tätige Personen im Ausland auf den Quellenschutz berufen (vgl. vorstehend E. 6.2.1 betreffend den persönlichen Schutzbereich von Art. 8 EMRK, wobei die Ausführungen auch für Art. 10 EMRK gelten). Zudem leitet der Beigeladene Informationen über Personen im Inland unverändert an die Vorinstanz weiter, wenn die Daten Informationen über eine konkrete Bedrohung der inneren Sicherheit enthalten beziehungsweise wenn die Vorinstanz aus eben diesem Grund die Entanonymisierung verlangt. Auch wenn dies gestützt auf ein überwiegendes öffentliches Interesse nicht von vornherein unzulässig ist, braucht es doch hinreichende verfahrensmässige Garantien beziehungsweise eine Absicherung, damit der Quellenschutz als Teilgehalt der Medienfreiheit beziehungsweise des Rechts auf Meinungsäusserung gewahrt und insbesondere die Verhältnismässigkeit von Beeinträchtigungen geprüft wird. Eine solche Garantie könnte in der Pflicht zur Aussonderung und Löschung entsprechender Daten bestehen, wobei eine solche hier weder im Gesetz noch in den Weisungen vorgesehen ist. Das anwendbare Recht enthält nach dem Gesagten keine (hinreichenden) Garantien, um den Quellenschutz zu gewährleisten. Dabei handelt es sich um einen gewichtigen Mangel. Um diesen zu beheben, wäre die (weitere) Bearbeitung von Kommunikation, die vertrauliches journalistisches Material enthält, unter den Vorbehalt der Genehmigung durch eine unabhängige (richterliche) Behörde zu stellen, die befugt ist, die Verhältnismässigkeit einer weiteren Bearbeitung zu überprüfen und verbindlich zu entscheiden (vgl. zit. Urteil Big Brother Watch und andere, § 450). Ein solcher Vorbehalt wäre für die Datenbearbeitung durch den Beigeladenen und durch die Vorinstanz erforderlich.

E. 16.3.6.3

Nach der Rechtsprechung des EGMR bestehen weitere Berufs- beziehungsweise Personengruppen, deren Kommunikationsbeziehungen einen besonderen Schutz der Vertraulichkeit verlangen. Dies gilt insbesondere für die Beziehung zwischen Anwalt und Mandant (vgl. vorstehend E. 6.2.1). Für Kommunikationsbeziehungen, die eines besonderen Schutzes bedürfen, enthält das Nachrichtendienstgesetz in Art. 58 Abs. 3 eine besondere Regelung: Betrifft die genehmigungspflichtige Beschaffungsmassnahme eine Person, die einer der in den Art. 171-173 StPO genannten Berufsgruppen angehört, erfolgt die Aussonderung und Vernichtung der Daten, die keinen Bezug zur spezifischen Bedrohungslange aufweisen, unter der Leitung des Bundesverwaltungsgerichts (vgl. zur grundsätzlich übereinstimmenden Rechtsprechung des deutschen Bundesverfassungsgerichts das zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, Ziff. 193 ff.). Die Bestimmung, die ohne weitere Erläuterungen im Rahmen der Beratung Eingang in das Nachrichtendienstgesetz gefunden hat, ist jedoch, wie bereits ausgeführt, nur auf genehmigungspflichtige Beschaffungsmassnahmen und damit auf die gezielte Überwachung, nicht jedoch im Rahmen der Massenüberwachung und damit nicht auf die Funk- und Kabelaufklärung anwendbar (vgl. auch vorstehend E. 6.3.4; zudem die Stellungnahme der Vorinstanz vom 11. November 2022, Beilage 2, S. 12 f.). Die Vorinstanz führt auch zum Schutz von Vertraulichkeitsbeziehungen aus, dass gemäss Art. 39 Abs. 3 NDG im Rahmen der Kabelaufklärung Angaben über schweizerische natürliche und juristische Personen und damit auch zu Rechtsanwälten als Suchbegriffe nicht zulässig seien. Damit bestehe bereits eine wesentliche Garantie zum Schutz vor Missbrauch. Ohnehin ergebe sich die Zuordnung zu einer Berufsgruppe und damit die Qualifikation der Kommunikation als besonders schützenswert grundsätzlich erst anhand des Inhalts der erfassten Kommunikation, wobei die Kommunikation mit E-Mail bei seriösen Providern verschlüsselt sei. Werde im Rahmen

der Analyse erkannt, dass es sich um schützenswerte Kommunikation handle, würden Angaben über Personen im Inland wiederum nur unter den Voraussetzungen von Art. 42 Abs. 2 und Abs. 3 NDG und damit grundsätzlich anonymisiert an die Vorinstanz weitergeleitet. Nach Ansicht der Vorinstanz wird damit dem Schutz von Vertraulichkeitsbeziehungen auch bei der Funk- und Kabelaufklärung ausreichend Rechnung getragen (Stellungnahme der Vorinstanz vom 12. April 2024, S. 9; Vernehmlassung der Vorinstanz vom 11. November 2022, Beilage 2, S. 13). Die von der Vorinstanz erwähnten Einschränkungen und Vorgaben (Art. 38 Abs. 4 Bst. b, Art. 39 Abs. 3 und Art. 42 Abs. 2 NDG) bieten grundsätzlich Schutz vor Missbrauch (vgl. vorstehend E. 16.3.2.1). Nach der Rechtsprechung des EGMR ist jedoch die Vertraulichkeit der Beziehung zwischen Rechtsanwalt und Mandant besonders zu schützen; es kommt ihr bei der Beurteilung der Notwendigkeit eines Eingriffs in das Privatleben erhöhtes Gewicht zu (vgl. vorstehend E. 6.2.1). Eine Pflicht zur Anonymisierung, die zudem auf Personen im Inland beschränkt ist (vgl. zum persönlichen Geltungsbereich von Art. 8 EMRK vorsehend E. 6.2.1 und E. 6.3.2), bietet hier keinen zusätzlichen beziehungsweise erhöhten Schutz vor Missbrauch. Im Rahmen von genehmigungspflichtigen Beschaffungsmassnahmen ist die Vorinstanz - weitergehend - zur Aussonderung und Vernichtung von besonders zu schützender Kommunikation verpflichtet. Aussonderung und Vernichtung haben zudem - zur Absicherung und damit als Massnahme zum Schutz vor Missbrauch - unter der Leitung des Bundesverwaltungsgerichts zu erfolgen (Art. 58 Abs. 3 NDG). Für Kommunikationen, die im Rahmen der Funk- und Kabelaufklärung erfasst worden sind und die, wie etwa die Kommunikation zwischen einem Rechtsanwalt und seinem Mandanten, eine besondere Vertraulichkeitsbeziehung betreffen, besteht kein vergleichbarer Schutz vor Missbrauch. Das Gesetz enthält keine Pflicht zur Aussonderung und Vernichtung entsprechender Daten und ihre weitere Verwendung steht auch nicht unter dem Vorbehalt der Beurteilung beziehungsweise Interessenabwägung durch eine unabhängige Behörde. Ein Ausgleich der widerstreitenden Interessen ist damit nicht abgesichert. Das Gesetz sieht somit betreffend Kommunikationsbeziehungen wie jene zwischen einem Rechtsanwalt und seinem Mandanten, die besonderen Schutz erfordern, keine ausreichenden Garantien zum Schutz vor Missbrauch vor. Es weist insofern einen Mangel auf. Gemäss der Rechtsprechung des EGMR ist nicht ausgeschlossen, dass dieser Mangel durch eine effektive, unabhängige und fortlaufende Überwachung der Massenüberwachung ausgeglichen werden kann (vgl. zit. Urteil Big Brother Watch und andere, § 408). Darauf wird im Rahmen der abschliessenden gesamthaften Beurteilung einzugehen sein (vgl. nachfolgend E. 25).

E. 16.4

Zusammenfassend ist zum vierten Prüfpunkt festzuhalten, dass das für die Auswahl, Auswertung und Verwendung des abgefangenen Materials einzuhaltende Verfahren in verschiedener Hinsicht nicht ausreichend vorhersehbar ist und zudem keine angemessenen Garantien gegen Missbrauch bietet. Zwar schränkt der Ausschluss rein inländischer Kommunikation von der Kabelaufklärung das Ermessen der Behörden erheblich ein und auch die organisatorische Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung ist eine wichtige Garantie zum Schutz vor Missbrauch. Insgesamt zeigt der vierte Prüfpunkt jedoch die folgenden Mängel auf: - Die Möglichkeit der Entanonymisierung von Informationen über Personen im Inland birgt insbesondere im Hinblick auf die Möglichkeit der Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an die Strafverfolgungsbehörden ein nicht unerhebliches Missbrauchspotential, ohne dass diesbezüglich eine verfahrensmässige Sicherung

vorhanden wäre (vgl. vorstehend E. 16.3.2.2). - Das anwendbare Recht enthält keine Pflicht, die Kabelaufklärung hinsichtlich der Aussonderung rein inländischer Kommunikation (technisch) kontinuierlich weiterzuentwickeln (vgl. vorstehend E. 16.3.2.3). - Es besteht keine hinreichende Gewähr, dass die Vorinstanz im Zusammenhang mit der Funk- und Kabelaufklärung nur richtige und erhebliche Daten bearbeitet (vgl. vorstehend E. 16.3.4.2). - Die Möglichkeit einer sogenannten Retrosuche beziehungsweise die damit verbundene Datenbearbeitung ist aufgrund des anwendbaren Rechts nicht in ausreichendem Mass vorhersehbar (vgl. vorstehend E. 16.3.4.4). - Das anwendbare Recht schreibt keine Protokollierung und Aufzeichnung aller Schritte der Massenüberwachung vor (vgl. vorstehend E. 16.3.5). - Das anwendbare Recht enthält keine Vorkehren, um den journalistischen Quellenschutz zu gewährleisten (vgl. vorstehend E. 16.3.6.2). - Es fehlen Garantien zum Schutz vor Missbrauch in Bezug auf Kommunikationsbeziehungen, die wie jene zwischen Rechtsanwalt und Mandat einen besonderen Schutz der Vertraulichkeit verlangen (vgl. vorstehend E. 16.3.6.3). Ob diese Mängel durch andere Garantien zum Schutz vor Missbrauch ausgeglichen werden können, ist im Rahmen der Gesamtbeurteilung zu prüfen (vgl. hierzu nachfolgend E. 25). Prüfpunkt 5 Die zu treffenden Vorkehrungen, wenn Material an andere Parteien übermittelt wird

E. 17.1

Die Grosse Kammer des EGMR hat in den beiden Urteilen Big Brother Watch und andere und Centrum för rättvisa die Vorkehren konkretisiert, die - zum Schutz vor Missbrauch - im Zusammenhang mit der Übermittlung von Informationen an andere Parteien vorzusehen sind. Der Gerichtshof ist der Ansicht, dass die Weitergabe von Informationen, die durch eine Massenüberwachung erlangt worden sind, an ausländische Staaten oder internationale Organisationen auf solche Informationen begrenzt werden sollte, die auf konventionskonforme Weise gesammelt und gespeichert wurden. Darüber hinaus seien in Bezug auf die Übermittlung von Informationen beziehungsweise Erkenntnissen aus einer Massenüberwachung an andere Parteien weitere Garantien zum Schutz vor Missbrauch vorzusehen. So müssten die Umstände, unter denen eine Übermittlung stattfinden darf, im innerstaatlichen Recht klar geregelt sein. Zudem habe der übermittelnde Staat sicherzustellen, dass der empfangende Staat beim Umgang mit den zu übermittelnden Daten Garantien eingerichtet hat, die geeignet sind, Missbrauch und einen unverhältnismässigen Eingriff in das Privatleben zu vermeiden; es muss insbesondere die sichere Aufbewahrung garantiert und die weitere Offenlegung der Informationen beschränkt sein. Diese Anforderungen bedeuten nicht notwendigerweise, dass der empfangende Staat einen vergleichbaren Schutz vorsehen muss wie der übermittelnde Staat. Verlangt ist vielmehr eine hinreichend sichere Aufbewahrung und eine Beschränkung der weiteren Offenlegung; die Grosse Kammer des EGMR verlangt insgesamt «des garanties suffisamment solides contre les abus» beziehungsweise «robust guarantees against abuse» (vgl. zit. Urteil Big Brother Watch und andere, § 399). Nicht erforderlich ist gemäss der Rechtsprechung des EGMR, dass vor jeder Übermittlung eine Zusicherung durch den empfangenden Staat abgegeben wird. Sollen jedoch Informationen übermittelt werden, die wie etwa journalistisches Material eine besondere Vertraulichkeit geniesst, sind besondere Garantien zum Schutz vor Missbrauch erforderlich. Schliesslich ist der EGMR der Ansicht, dass die Übermittlung von Material an ausländische Partner der Kontrolle durch eine unabhängige Behörde unterliegen sollte (zit. Urteile Big Brother Watch und andere, § 362 und Centrum för rättvisa, § 276). In seinem Urteil Big Brother Watch und andere kam die Grosse Kammer des EGMR zum Ergebnis, dass das damalige im Vereinigten Königreich

anwendbare Recht hinreichende Garantien gegen Missbrauch enthielt. So war die Übermittlung auf das zur Erfüllung der jeweiligen Aufgabe Notwendige beschränkt (sog. «'need-to-know' principle» bzw. «principe du 'besoin d'en connaître'»; vgl. hierzu zit. Urteil Big Brother Watch und andere, § 393). Zudem konnten nach damaligem Recht bestimmte Partnerdienste direkt auf die Systeme des Nachrichtendienstes des Vereinigten Königreichs zugreifen, womit gewährleistet war, dass ein Zugang nur zu rechtmässig beschafften Informationen bestand. In Fällen, in denen Informationen an einen anderen Dienst ausserhalb des Vereinigten Königreichs weitergegeben wurden, war sicherzustellen, dass der betreffende Dienst über die erforderlichen Verfahren zum Schutz der Informationen verfügt und diese auch beibehalten werden. Zudem war zu gewährleisten, dass die Informationen nur im erforderlichen Mass weitergegeben, kopiert, verteilt und aufbewahrt werden. Die Geheimdienstpartner mussten mithin für die sichere Aufbewahrung von übermittelten Informationen sorgen und seine weitere Offenlegung einschränken. Zudem war eine unabhängige Kontrolle vorgesehen (vgl. hierzu nachfolgend E. 19.1 und 22.2.1). Schliesslich waren Informationen, die eine besondere Vertraulichkeit genossen, entsprechend zu kennzeichnen und im Falle von Zweifeln an der Rechtmässigkeit der Weitergabe war eine interne Kontrollstelle zu Rate zu ziehen. Die genannten Vorgaben waren in einer verbindlichen Richtlinie festgehalten (vgl. zit. Urteil Big Brother Watch und andere, §§ 392 ff.). In seinem Urteil Centrum för rättvisa wies die Grosse Kammer des EGMR zunächst anerkennend auf die Bedeutung der internationalen Zusammenarbeit bei der Aufdeckung und Bekämpfung von Bedrohungen für die nationale Sicherheit hin. Entsprechend könne aus verschiedenen Gründen die Notwendigkeit entstehen, ausländischen Diensten Erkenntnisse zu übermitteln, die durch die Massenüberwachung des Fernmeldeverkehrs gewonnen worden seien. Die Gründe seien zudem nicht vorhersehbar und könnten daher nicht abschliessend gesetzlich festgelegt werden; eine gewisse Offenheit der gesetzlichen Regelung zur Übermittlung von Informationen an andere Parteien sei daher hinzunehmen. Ohnehin sei die Massenüberwachung des Fernmeldeverkehrs von durchgehenden Garantien zum Schutz vor Missbrauch zu begleiten, was jedenfalls in einem gewissen Rahmen auch die nachteiligen Folgen einer Übermittlung von Erkenntnissen an andere Stellen zu begrenzen vermöge. Das anwendbare Recht erlaubte die Übermittlung von Erkenntnissen an ausländische Partner. Eine Pflicht, die Notwendigkeit und (damit) die Verhältnismässigkeit der Übermittlung von Erkenntnissen im Einzelfall zu überprüfen, bestand jedoch nicht. Zudem war der schwedische Dienst nicht gesetzlich verpflichtet, fest- und sicherzustellen, ob und dass der ausländische Empfänger in hinreichendem Mass die Sicherheit der übermittelten Daten zu gewährleisten und Missbrauch zu begrenzen vermag. Der Gerichtshof erkannte darin einen erheblichen Mangel der schwedischen Regelung zur Massenüberwachung des Fernmeldeverkehrs (vgl. zit. Urteil Centrum för Rättvisa, §§ 321-330). In Bezug auf die Bekanntgabe von Erkenntnissen aus der Massenüberwachung an Behörden im Inland kam der Gerichtshof in beiden Urteilen zum Ergebnis, dass das damals anwendbare nationale Recht mit der Beschränkung der Bekanntgabe auf das Notwendige in hinreichendem Mass Schutz vor Missbrauch bot (vgl. zit. Urteile Big Brother Watch und andere, §§ 392-394 und Centrum för rättvisa, § 317).

E. 17.2

Im Nachrichtendienstgesetz ist zunächst die Bekanntgabe von Personendaten an inländische Behörden geregelt. Demnach gibt die Vorinstanz Personendaten inländischen Behörden bekannt, wenn dies zur Wahrung der inneren oder äusseren Sicherheit notwendig ist. Der Bundesrat bestimmt die betreffenden Behörden (Art. 60 Abs. 1 NDG; vgl. zu den

betreffenden Behörden Art. 32 Abs. 1 NDV und Anhang 3 zur NDV). Die Bekanntgabe ist zudem zu protokollieren; gemäss Art. 32 Abs. 3 NDV registriert die Vorinstanz die Bekanntgabe, die Empfängerin oder den Empfänger, den Gegenstand und den Grund. Schliesslich untersagt Art. 32 Abs. 4 NDV die Bekanntgabe von Personendaten, wenn ihr überwiegende öffentliche oder private Interessen entgegenstehen. Letzteres verlangt im Ergebnis nach einer Prüfung im Einzelfall. Gemäss Art. 61 Abs. 1 NDG kann die Vorinstanz sodann Personendaten oder Listen von Personendaten ins Ausland bekannt geben, wobei sie vor jeder Bekanntgabe prüft, ob die rechtlichen Voraussetzungen für die Bekanntgabe erfüllt sind. Dabei ist - in Anwendung von Art. 16 Abs. 1 DSG - sicherzustellen, dass die Gesetzgebung des Empfängerstaates einen angemessenen Datenschutz gewährleistet; gemäss Art. 16 Abs. 1 DSG dürfen Personendaten ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Datenschutz gewährleistet. In diesem Fall ist grundsätzlich auch eine Bekanntgabe im Abrufverfahren möglich (vgl. Art. 61 Abs. 4 NDG). Bei der Prüfung, ob die Gesetzgebung des Empfängerstaates angemessen ist, hat der Bundesrat die Kriterien gemäss Art. 8 Abs. 2 der Datenschutzverordnung (DSV, SR 235.11) zu berücksichtigen, das heisst etwa in grundsätzlicher Weise die Rechtsstaatlichkeit und die Achtung der Menschenrechte sowie in spezifischer Hinsicht die geltende Gesetzgebung insbesondere zum Datenschutz, einschliesslich der wirksamen Gewährleistung der Rechte von betroffenen Personen. Die Ergebnisse der Prüfungen durch den Bundesrat werden im Anhang zur Datenschutzverordnung veröffentlicht (Art. 8 Abs. 1 DSV). Der Anhang der DSV ist als Positiv-Liste konzipiert und enthält eine Auflistung jener Staaten, deren Gesetzgebungen einen angemessenen Datenschutz sicherstellen. Gewährleistet die Gesetzgebung des Empfängerstaates keinen angemessenen Datenschutz, so können Personendaten diesem Staat in Abweichung von Art. 16 Abs. 1 DSG bekannt gegeben werden, wenn die Schweiz zu diesem Staat diplomatische Beziehungen pflegt und eine der in Art. 61 Abs. 2 NDG genannten Voraussetzungen erfüllt ist, das heisst wenn etwa eine gesetzliche oder völkerrechtliche Verpflichtung zur Bekanntgabe besteht oder die Bekanntgabe zur Wahrung eines überwiegenden öffentlichen Sicherheitsinteresses notwendig ist. Gemäss Art. 61 Abs. 5 NDG dürfen Personendaten einem ausländischen Sicherheitsorgan nicht bekannt gegeben werden, wenn die betroffene Person dadurch der Gefahr einer Doppelbestrafung oder ernsthafter Nachteile für Leib, Leben oder Freiheit im Sinne der EMRK oder anderer, von der Schweiz ratifizierter internationaler Abkommen ausgesetzt wird.

E. 17.3.1

Die Beurteilung, ob das anwendbare Recht in Bezug auf die Übermittlung von Erkenntnissen an Dritte hinreichende Vorkehrungen zum Schutz vor Missbrauch enthält, ist gemäss der Rechtsprechung des EGMR auf folgende Kriterien abzustützen: - Beschränkung der Übermittlung auf rechtmässig erhobene Daten - Beschränkung der Übermittlung auf das Notwendige - Gewährleistung eines hinreichenden Datenschutzes im Empfängerstaat - Vorkehren zum Schutz von vertraulicher Kommunikation - Unabhängige Kontrolle der Übermittlung von Erkenntnissen

E. 17.3.2

Das anwendbare Recht schränkt sowohl die Behörden im Inland, an welche Personendaten bekannt gegeben werden dürfen, als auch den Umfang der Bekanntgabe ein; die Bekanntgabe ist gemäss Art. 60 Abs. 1 NDG zulässig, soweit sie zur Wahrung der inneren

oder äusseren Sicherheit notwendig ist. Die Regelung birgt keine besondere Gefahr von Missbrauch (vgl. zur Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an die Strafverfolgungsbehörden vorstehend E. 16.3.4.3).

E. 17.3.3

Die Bekanntgabe von Personendaten und damit auch die Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an ausländische Behörden ist in Art. 61 Abs. 1 NDG ausdrücklich vorgesehen. Zudem wird ersichtlich, dass die Bekanntgabe grundsätzlich unter dem Vorbehalt der Gewährleistung eines angemessenen Datenschutzes im Empfängerstaat steht (vgl. Art. 61 Abs. 2 NDG). Das anwendbare Recht ist insoweit in hinreichendem Mass vorhersehbar. Es schreibt sodann vor, dass der Bundesrat nach bestimmten Kriterien prüft, ob der Empfängerstaat einen angemessenen Datenschutz gewährleistet und die Vorinstanz prüft vor jeder Bekanntgabe, ob die rechtlichen Voraussetzungen für die Bekanntgabe erfüllt sind; die Angemessenheit des Datenschutzes wird periodisch neu beurteilt (Art. 8 Abs. 4 DSV). Das Verordnungsrecht gibt in Art. 8 Abs. 2 DSV zwar die Kriterien, jedoch keinen Massstab zur Beurteilung der Angemessenheit des im Empfängerstaat geltenden Rechts vor. Auch aus den Materialien ist nicht ersichtlich, was der Beurteilungsmassstab ist. Entsprechend ist nicht ohne Weiteres (hinreichend) gewährleistet, dass der empfangende Staat eine sichere Aufbewahrung des Materials garantiert und eine weitere Offenlegung beschränkt - oder in genereller Weise einen mit dem inländischen Recht vergleichbaren Datenschutz gewährleistet. Darüber, ob die Praxis des Bundesrates, der bei jeder Beurteilung den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB konsultiert (Art. 8 Abs. 3 DSV), in eben diese Richtung geht, liegen dem Bundesverwaltungsgericht keine Angaben vor. Jedenfalls vermag der Mangel hier mit Blick auf den Kriterienkatalog von Art. 8 Abs. 2 DSV nicht allzu schwer zu wiegen und es ist davon auszugehen, dass gestützt auf die Beurteilung gemäss Art. 16 Abs. 1 DSG und Art. 8 DSV grundsätzlich eine sichere Aufbewahrung der Daten und ein Schutz vor einer missbräuchlichen Datenbearbeitung im Empfängerstaat gewährleistet ist. Nach der Rechtsprechung des EGMR ist die Übermittlung beziehungsweise Bekanntgabe zudem auf das Notwendige zu beschränken. Dabei handelt es sich um eine wichtige Massnahme zur Begrenzung der Datenübermittlung und damit zum Schutz vor Missbrauch. So verpflichtet die Einschränkung der Datenübermittlung auf das Notwendige zunächst den Empfängerstaat, sein Bedürfnis und damit auch den Zweck der Übermittlung offen zu legen beziehungsweise zu begründen. Im Weiteren ist der übermittelnde Staat verpflichtet, die Bekanntgabe im Hinblick auf ein legitimes Bedürfnis zu überprüfen und in diesem Sinne zu rechtfertigen. Auf diese Weise würde die Übermittlung von Erkenntnissen aus der Funk- und Kabelaufklärung im Rahmen der Kontrolle durch eine unabhängige Behörde überprüfbar. Ein solcher Schutz beziehungsweise eine solche Hürde für die Übermittlung von Daten fehlt hier; das anwendbare Recht schreibt anders als für die Bekanntgabe von Personendaten an inländische Behörden (vgl. Art. 60 Abs. 1 NDG) nicht vor, dass die Bekanntgabe auf das Notwendige zu beschränken ist und die Vorinstanz äusserte sich auch nicht zu diesem Punkt. Ferner sind keine besonderen Garantien vorgesehen für den Fall, dass Daten, die wie etwa journalistisches Material eine besondere Vertraulichkeit verlangen, übermittelt werden sollen. Das anwendbare Recht bietet insofern keinen hinreichenden Schutz vor Missbrauch. Ob diese Mängel durch andere Vorkehren zum Schutz vor Missbrauch ausgeglichen werden kann, wird im Rahmen der gesamthaften Beurteilung zu entscheiden sein. Die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND, auf die an anderer Stelle noch einzugehen sein

wird (vgl. nachfolgend E. 19-21), hat im Rahmen ihres Prüfplans im Jahr 2024 die Organisation der Partnerdienstkontakte überprüft. Sie führte hierzu neun Interviews durch. In ihrem Tätigkeitsbericht für das Jahr 2024 hält sie fest, dass die Partnerdienstkontakte vom Beigeladenen im Auftrag der Vorinstanz durchgeführt würden, wirksam organisiert seien und sich der Beigeladene zudem «an die gesetzlichen Vorgaben» halte (vgl. Tätigkeitsbericht der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND für das Jahr 2024, S. 8 f., < www.ab-nd.admin.ch > Tätigkeitsberichte, abgerufen am 16. Oktober 2025). Ob einzelne Partnerkontakte beziehungsweise die Übermittlung von Daten im Einzelfall überprüft worden sind, ergibt sich aus den Tätigkeitsberichten der Aufsichtsbehörde nicht. Die Aufsichtstätigkeit der Behörde scheint mithin, soweit für das Bundesverwaltungsgericht beurteilbar, nicht auf die (stichprobenweise) Überprüfung der einzelnen Datenbearbeitung, sondern vielmehr auf die Erkennung grundsätzlicher Probleme ausgerichtet zu sein (vgl. hierzu und zur Bewertung dieses Kriteriums auch nachfolgend E. 21.2.3).

E. 17.4

Zusammenfassend ergibt sich zum Prüfpunkt 5, dass die Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an inländische Behörden auf das Notwendige beschränkt und somit das Ermessen der Vorinstanz in hinreichendem Mass eingeschränkt ist. Die Übermittlung an Behörden im Ausland ist sodann nur zulässig, wenn die Gesetzgebung des Empfängerstaates einen angemessenen Datenschutz gewährleistet. Die Kriterien zur Beurteilung der Angemessenheit sind im Gesetz indes nicht in hinreichendem Mass verbindlich vorgegeben. Zudem ist die Übermittlung an Behörden im Ausland nicht von Gesetzes wegen auf das Notwendige beschränkt und es sind keine besonderen Garantien zum Schutz von Kommunikationsbeziehungen vorgesehen, die besonderen Schutz geniessen. Schliesslich ist nicht ersichtlich, dass im Rahmen einer unabhängigen nachträglichen Kontrolle konkrete Datenübermittlungen zumindest stichprobenweise überprüft würden. Damit fehlen fehlt insgesamt eine wichtige Begrenzung und Rechtfertigung der Bekanntgabe ins Ausland. Ob die Mängel ausgeglichen werden können, wird im Rahmen der Gesamtbeurteilung zu entscheiden sein (vgl. nachfolgend E. 25). Prüfpunkt 6 Die Grenzen für die Dauer der Überwachung und Aufbewahrung von abgefangenem Material und die Umstände, unter denen solches Material gelöscht und zerstört werden muss

E. 18.1

Nach der Rechtsprechung des EGMR muss das nationale Recht auch im Zusammenhang mit der Dauer einer Überwachung und der Aufbewahrung von Daten hinreichende Garantien zum Schutz vor Missbrauch enthalten. Zudem ist verbindlich vorzuschreiben, unter welchen Umständen beziehungsweise zu welchem Zeitpunkt die Daten (automatisch) zu löschen sind. Erforderlich ist demnach eine ausreichend klare und damit vorhersehbare Regelung im innerstaatlichen Recht über den Zeitraum, während dem eine Überwachung zulässig ist, die Dauer, für die eine Überwachung verlängert werden kann, und die Umstände, unter denen eine Überwachung beendet werden muss. Zur Begrenzung einer Überwachung auf das Notwendige ist zudem verpflichtend vorzuschreiben, dass diese fortlaufend auf ihre Erforderlichkeit hin überprüft wird (vgl. zit. Urteile Centrum för rättvisa, § 331 und Big Brother Watch und andere, § 401). Im Weiteren muss das nationale Recht zumindest («au minimum» bzw. «as a very minimum») vorschreiben, dass Daten zu löschen sind, wenn sie für die nachrichtendienstliche Tätigkeit keine Bedeutung mehr

haben (zit. Urteil Centrum för rättvisa, § 342). (Hierzu) sollte die Notwendigkeit der weiteren Speicherung von erfassten Daten (Kommunikations- und Randdaten) regelmässig überprüft werden (zit. Urteil Centrum för rättvisa, § 343). Gemäss den Sachverhalten, die den beiden Urteilen Big Brother Watch und andere und Centrum för rättvisa zu Grunde lagen, war die Genehmigung zur Durchführung einer Überwachung jeweils auf (längstens) sechs Monate beschränkt. Zudem bestand die Möglichkeit, die Überwachung für jeweils sechs weitere Monate zu verlängern. Insoweit enthielt das (damals) anwendbare Recht hinreichende Garantien gegen Missbrauch (vgl. zit. Urteile Big Brother Watch und andere, §§ 400 f. und Centrum för rättvisa, §§ 331 f.). Hingegen schrieb das schwedische Recht nicht vor, dass eine Überwachung zu beenden ist, sobald die Voraussetzungen hierfür nicht mehr gegeben sind beziehungsweise die Massnahme nicht mehr erforderlich ist. Der Gerichtshof mass diesem Mangel angesichts weiterer Massnahmen zum Schutz vor Missbrauch - insbesondere der fortlaufenden Überwachung durch die Aufsichtsbehörde - nicht allzu viel Gewicht bei (zit. Urteil Centrum för rättvisa, §§ 333-336). Schliesslich erachtete es der Gerichtshof noch als angemessen, dass die erfassten Kommunikationen und die Randdaten bis zu zwei Jahren aufbewahrt werden, wobei das damals im Vereinigten Königreich anwendbare Recht vorschrieb, dass für das Löschen von Daten nach Ablauf der Aufbewahrungsfrist so weit als möglich ein Prozess der automatischen Löschung vorzusehen ist (zit. Urteil Big Brother Watch und andere, §§ 402-405; vgl. auch zit. Urteil Centrum för rättvisa, § 343).

E. 18.2.1

Aufträge zur Kabelaufklärung sind gemäss Art. 40 Abs. 1 NDG genehmigungspflichtig. Erteilt das Bundesverwaltungsgericht die Genehmigung, so gilt diese für höchstens sechs Monate (Art. 41 Abs. 3 Satz 1 NDG). Die Genehmigung kann sodann nach demselben Verfahren um jeweils höchstens drei Monate verlängert werden (Art. 41 Abs. 3 Satz 2 NDG). Die Beschaffungsmassnahme ist unverzüglich zu beenden, wenn die Frist abgelaufen ist oder die Voraussetzungen für eine weitere Durchführung nicht mehr erfüllt sind (Art. 32 Abs. 1 Bst. a und b NDG). Die Dauer, während der eine Funkaufklärung zulässig ist, wird nicht begrenzt. Die maximale Aufbewahrungsdauer der erfassten Kommunikationen und der erfassten Randdaten ist im Verordnungsrecht geregelt (Art. 38 Abs. 3 und Art. 39 Abs. 4 Bst. c NDG). Demnach vernichtet der Beigeladene die Daten im Zeitpunkt der Beendigung des Auftrags, spätestens aber 18 Monate (Kommunikationen) beziehungsweise fünf Jahre (Randdaten) nach deren Erfassung (Art. 28 Abs. 2 und 3 NDV, Art. 4 Abs. 2 und 3 VEKF). Die im Rahmen der Funk- und Kabelaufklärung gewonnene Resultate vernichtet der Beigeladene spätestens im Zeitpunkt der Beendigung des betreffenden Auftrags (Art. 28 Abs. 1 NDV, Art. 4 Abs. 1 VEKF). In Art. 39 Abs. 2 NDG ist schliesslich vorgeschrieben, dass rein schweizerische Kommunikation zu vernichten ist, sobald erkannt wird, dass es sich um solche handelt (vgl. für die Funkaufklärung Art. 5 VEKF, wobei die Regelung gemäss Art. 5 Abs. 1 VEKF in einem gewissen Widerspruch zu den Möglichkeiten der Entanonymisierung und Retrosuche stehen). Die Vorinstanz erfasst die Resultate aus der Funk- und Kabelaufklärung praxisgemäss im integralen Analysesystem (IASA NDB) oder, wenn eine Zuweisung zum integralen Analysesystem (IASA NDB) noch nicht möglich ist, im Restdatenspeicher; im Zusammenhang mit der Bearbeitung von Gesuchen um Verlängerung der Genehmigung eines Auftrags zur Kabelaufklärung werden die Resultate zudem im Informationssystem zur Geschäftsverwaltung des NDB (GEVER NDB) bearbeitet (vgl. vorstehend E. 16.2.2). Gemäss Art. 8 VIS-NDB löscht die Vorinstanz die Daten in ihren Informations- und

Speichersystemen innerhalb von drei Monaten nach Ablauf der jeweiligen Aufbewahrungsdauer, wobei danach differenziert wird, ob es sich um ein Original- oder ein Quellendokument handelt (Abs. 2; vgl. auch Art. 8 Abs. 3 und Abs. 5 VIS-NDB). Die Aufbewahrungsdauer für Daten im integralen Analysesystem (IASA NDB) ist in Art. 21 VIS-NDB geregelt. Sie beträgt für Originaldokumente, die nicht mit einem Quellendokument referenziert sind, höchstens 15 Jahre (Art. 21 Abs. 2 VIS-NDB) und für Quellendokumente je nach Bereich bis zu 45 Jahre (Art. 21 Abs. 1 VIS-NDB; vgl. für das Informationssystem zur Geschäftsverwaltung des NDB [GEVER NDB] Art. 40 VIS-NDB, für das Informationssystem Kommunikationsaufklärung [ISCO] Art. 60 VIS-NDB und für den Restdatenspeicher Art. 65 VIS-NDB). Die Verordnung schreibt für das integrale Analysesystem (IASA NDB) zudem vor, dass die für die Datenerfassung zuständigen Mitarbeiterinnen und Mitarbeiter Personendatensätze innerhalb bestimmter Fristen insbesondere auf ihre Erforderlichkeit hin überprüfen und nicht mehr benötigte Daten löschen (Art. 20 VIS-NDB).

E. 18.2.2

Die Vorinstanz und der Beigeladene äussern sich insbesondere im Rahmen ihrer Antworten zu den Fragenkatalogen des Bundesverwaltungsgerichts dazu, wie sie die Vorgaben bezüglich Aufbewahrungsdauer und Löschung in der Praxis anwenden. Der Beigeladene hält fest, seine Datenbearbeitung sei so konfiguriert, dass erfasste Kommunikationen und Randdaten bei Ablauf der im Verordnungsrecht festgelegten Fristen automatisch und unwiderruflich «überschrieben» würden. In der Praxis gehe eine limitierende Wirkung auch von den zur Verfügung stehenden Kapazitäten aus; die im Rahmen der Kabelaufklärung erfassten Signale würden durchschnittlich während drei bis vier Monate aufbewahrt (Stellungnahme des Beigeladenen vom 10. November 2022, S.12). Die Vorinstanz weist zunächst darauf hin, dass sich die zulässige maximale Aufbewahrungsdauer je nach Informationssystem unterscheide. Für die Berechnung der maximalen Aufbewahrungsdauer sei sodann das Datum der Ablage eines Dokuments entscheidend. Bei Originaldokumenten, die nicht mit einem Quellendokument verknüpft seien, sei das Datum der Ablage des Originaldokuments fristauslösend. Sei das Dokument demgegenüber mit einem Quellendokument verknüpft, sei für die Bestimmung der Aufbewahrungsfrist das Datum, an welchem das Quellendokument erstellt worden sei, massgebend. Eine Richtlinie im Zusammenhang mit der Bestimmung der maximalen Aufbewahrungsdauer bestehe nicht. Weiter sei zwischen dem Löschen und dem Vernichten von Daten zu unterscheiden. Die im Informationssystem zur Geschäftsverwaltung des NDB (GEVER NDB), im Informationssystem Kommunikationsaufklärung (ISCO) und im integralen Analysesystem (IASA NDB) beziehungsweise im Restdatenspeicher erfassten Daten würden, wenn sie nicht mehr benötigt würden oder die maximal zulässige Aufbewahrungsdauer abgelaufen sei, in den Informationssystemen der Vorinstanz gelöscht. Das Löschen werde weisungsgemäss protokolliert und erfolge im integralen Analysesystem (IASA NDB) automatisch, während in den Informationssystemen zur Geschäftsverwaltung des NDB (GEVER NDB) und Kommunikationsaufklärung (ISCO) die Daten regelmässig auch in Bezug auf ihre Aufbewahrungsdauer hin überprüft und manuell gelöscht würden. Die betreffenden Daten (Kommunikationen und Randdaten) würden mit dem Löschen jedoch nicht vernichtet, sondern nach dem Löschen gemäss der Vorgabe von Art. 68 Abs. 1 NDG dem Schweizerischen Bundesarchiv BAR zur Übernahme angeboten. Bis zur Übernahme durch das Schweizerische Bundesarchiv BAR könnten gelöschte Daten wiederhergestellt werden, da sie bis zum betreffenden Entscheid gesondert aufbewahrt und erst nach der

Übergabe physisch gelöscht würden. Werde demgegenüber ihm Rahmen der Beurteilung etwa der Richtigkeit und Erheblichkeit eines Resultats festgestellt, dass beispielsweise kein hinreichender Aufgabenbezug vorliege oder eine Datenbearbeitungsschranke verletzt sei, würden die betreffenden Daten vernichtet oder unwiderruflich anonymisiert. Auch die Vernichtung werde weisungsgemäss protokolliert. Sie erfolge zudem endgültig, könne also nicht rückgängig gemacht werden. Eine Übergabe an das Schweizerische Bundesarchiv BAR erfolge in diesem Fall nicht (Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 14 ff. [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 2. September 2025] und S. 16 f.; Stellungnahme der Vorinstanz vom 22. November 2022, Beilage 2, S. 21 f. und 24 f.).

E. 18.3.1

Die Beurteilung, ob das anwendbare Recht die Dauer der Überwachung und die Aufbewahrung der erfassten Daten in hinreichendem Mass begrenzt, ist gemäss der dargestellten Rechtsprechung des EGMR auf die folgenden Kriterien abzustützen: - Zeitliche Begrenzung der Überwachung - Umstände, unter denen eine Überwachung beendet werden muss - Zeitliche Begrenzung der Aufbewahrung der Daten - Pflicht zur Löschung der Daten

E. 18.3.2

Die Dauer, während der eine Kabelaufklärung durchgeführt werden darf, ist im Gesetz klar begrenzt: Gemäss Art. 41 Abs. 3 NDG gilt die Genehmigung des Bundesverwaltungsgerichts für höchstens sechs Monate. Sie kann zudem um jeweils höchstens drei Monate verlängert werden. Es besteht insoweit in Bezug auf die Kabelaufklärung eine ausreichend vorhersehbare und hinreichende Garantie gegen Missbrauch (vgl. zur beabsichtigten Ausdehnung der zeitlichen Begrenzung kritisch vorstehend E. 14.4.3). Demgegenüber ist die Dauer eines Auftrags zur Funkaufklärung weder im Gesetz noch in der Verordnung begrenzt und das anwendbare Recht bietet insoweit keinen hinreichenden Schutz vor Missbrauch (vgl. zusätzlich zu den zit. Urteilen Big Brother Watch und andere und Centrum för rättvisa BGE 149 I 218 E. 8.3.2). Dieser Mangel wiegt mit Blick darauf, dass für einen Auftrag auch keine vorgängige Überprüfung beziehungsweise Genehmigung erforderlich ist, schwer. Das anwendbare Recht enthält sodann keine (spezifische) Regelung zur (vorzeitigen) Beendigung einer Funk- oder Kabelaufklärung. Zwar schreibt die Bestimmung von Art. 32 NDG unter anderem vor, dass die Massnahme zu beenden ist, wenn die Voraussetzungen für eine weitere Durchführung nicht mehr erfüllt sind. Die Bestimmung, die ohnehin nur für die Kabelaufklärung anwendbar ist (vgl. Art. 41 Abs. 2 NDG), vermag jedoch hier keine limitierende Wirkung zu entfalten; die «Voraussetzungen» für die Kabelaufklärung sind im Gesetz, dessen Natur als strategisches Aufklärungsmittel entsprechend, final formuliert (vgl. Art. 39 Abs. 1 NDG, wonach die Kabelaufklärung zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland eingesetzt werden kann). (Entsprechend) schreibt das Gesetz auch nicht verpflichtend vor, die Aufträge zur Überwachung fortlaufend auf ihre Erforderlichkeit hin zu überprüfen. Weder die Funk- noch die Kabelaufklärung wird insoweit durch das Gesetz (in hinreichendem Mass) auf das Notwendige beschränkt; immerhin ergibt sich für die Kabelaufklärung aus der zeitlichen Begrenzung der Gültigkeit der Genehmigung, dass die Kabelaufklärung (jedenfalls) mit Ablauf der Gültigkeit der Genehmigung zu beenden ist (ausdrücklich auch Art. 32 Abs. 1 Bst. a NDG). Vor Ablauf der Dauer einer Genehmigung liegt es mithin im Ermessen der

Vorinstanz, eine Überwachung vorzeitig zu beenden, sobald diese nicht mehr erforderlich ist oder die Umstände sich wesentlich geändert haben. Dieser Mangel kann nach der dargestellten Rechtsprechung des EGMR durch eine fortlaufende und effektive Überwachung durch die Aufsichtsbehörde ausgeglichen werden (vgl. zit. Urteil Centrum för rättvisa, §§ 335 f.). Darauf wird im Rahmen der gesamthaften Beurteilung unter Berücksichtigung der Ergebnisse zu Prüfpunkt 7 zurückzukommen sein (vgl. nachfolgend E. 25). Im Weiteren ist die maximale Dauer, während der der Beigeladene die Daten (erfasste Kommunikationen und Randdaten) aufbewahren darf, in Art. 28 NDV und Art. 4 VEKF verbindlich festgelegt. Demnach vernichtet der Beigeladene die Daten und Resultate im Zeitpunkt der Beendigung des Auftrags, spätestens aber nach 18 Monaten (Kommunikationen) beziehungsweise nach fünf Jahren (Randdaten). Zwar erscheint fraglich, ob die Verordnungsbestimmungen den gesetzlichen Vorgaben gemäss Art. 38 Abs. 6 und Art. 42 Abs. 4 NDG entsprechen. Mit Blick auf die Rechtsprechung des EGMR erscheint jedoch die Begrenzung der Aufbewahrungsdauer für erfasste Kommunikationen auf 18 Monate und die Pflicht zur Löschung nach Ablauf der Frist als angemessen; der EGMR hat eine Aufbewahrung über zwei Jahre als mit Art. 8 EMRK vereinbar bezeichnet. Näher einzugehen ist auf die maximale Aufbewahrungsdauer für Randdaten (vgl. in diesem Zusammenhang auch das vor dem EGMR hängige Verfahren Balthasar Glättli gegen die Schweiz, 47351/18, betreffend die Pflicht der Fernmeldedienstanbieterinnen zur Speicherung von Randdaten der Telekommunikation). Die Randdaten enthalten Informationen darüber, wer mit wem, wann, wie lange und von wo aus kommuniziert hat (vgl. vorstehend E. 6.2.1). In einer Zeit, in der überwiegend auf elektronischem Weg kommuniziert wird, können die Randdaten der Kommunikation Rückschlüsse auf die persönlichen Lebensverhältnisse und das persönliche Umfeld zulassen. Hier fällt jedoch massgebend in Betracht, dass die Kabelaufklärung - anders als genehmigungspflichtige Beschaffungsmassnahmen - nicht zielgenau ist. Insofern ist jedenfalls nicht sehr wahrscheinlich, dass im Rahmen einer Kabelaufklärung grosse Teile der Kommunikation der Beschwerdeführenden erfasst werden und so entsprechende Rückschlüsse ohne Weiteres möglich wären. Auch die maximale Aufbewahrungsdauer von fünf Jahren für Randdaten der Kommunikation erscheint aufgrund der Trennung von Vorinstanz und Beigeladenen sowie trotz der Möglichkeit der Retrosuche insgesamt noch als angemessen (vgl. demgegenüber zit. Urteil Big Brother Watch und andere, § 423). Die dargestellte Rechtsprechung es EGMR bezieht sich auf die Aufbewahrung der Daten (erfasste Kommunikationen einschliesslich der Randdaten) durch den Beigeladenen (vgl. zit. Urteil Centrum för rättvisa, § 343, in welchem die Daten als «les éléments interceptés non traités» beziehungsweise «unprocessed intercept material» bezeichnet werden). Zu der Frage, wie lange Resultate der Kabelaufklärung aufbewahrt werden dürfen, musste sich der EGMR bisher nicht äussern. Hier ist davon auszugehen, dass das Aufbewahren von Resultaten aus der Kabelaufklärung durch die Vorinstanz ebenfalls zum Regime der Massenüberwachung gehört. Es ist daher auch zu prüfen, ob die Aufbewahrungsdauer, wie sie das Verordnungsrecht für die nachrichtendienstlichen Informationssysteme vorschreibt (vgl. vorstehend E. 18.2.1), angemessenen Schutz vor Missbrauch bietet. Die Resultate aus der Funk- und Kabelaufklärung werden hauptsächlich im integralen Analysesystem (IASA NDB) bearbeitet. Das Verordnungsrecht legt für Daten, die im integralen Analysesystem (IASA NDB) bearbeitet werden, unterschiedliche Aufbewahrungsfristen fest. Diese unterscheiden sich je nachdem, ob es sich um Original- oder Quellendokumente handelt. Bei Quellendokumenten ist bezüglich der Aufbewahrungsdauer sodann zusätzlich

thematisch zu unterscheiden (vgl. Art. 21 Abs. 1 VIS-NDB). Wie sich die Aufbewahrungsfrist im Einzelnen berechnet beziehungsweise welche Datenbearbeitung für die Bestimmung der maximal zulässigen Aufbewahrungsdauer massgebend ist, kann auch gestützt auf die Erläuterungen der Vorinstanz zu den Fragenkatalogen nicht abschliessend nachvollzogen werden. So handelt es sich bei Quellendokumenten gemäss den Angaben der Vorinstanz lediglich um eine technische Verbindungsstelle zwischen einem Objekt und einem Originaldokument, die aber auch weitere Informationen wie etwa die Zusammenfassung des Inhalts eines Originaldokuments enthalten kann. Es ist davon auszugehen, dass Quellendokumente fortlaufend geändert beziehungsweise ergänzt werden, indem etwa zusätzliche Verknüpfungen zu Originaldokumenten oder Objekten erstellt und (so) neue Erkenntnisse gewonnen werden. Vor diesem Hintergrund bleibt etwa unklar, ob sich die maximale Aufbewahrungsdauer für Quellendokumente nach dem Zeitpunkt der erstmaligen strukturierten Erfassung bestimmt oder ob spätere Änderungen wie etwa zusätzliche Verknüpfungen die maximal zulässige Aufbewahrungsdauer verlängern. Eine erläuternde beziehungsweise konkretisierende Richtlinie oder eine interne Weisung zur Umsetzung der gesetzlichen Vorgaben zur Aufbewahrungsdauer von Daten im integralen Analysesystem (IASA NDB) besteht gemäss den Angaben der Vorinstanz nicht (Stellungnahme der Vorinstanz vom 28. November 2023, Beilage 30, S. 16). Zusätzlich fällt in Betracht, dass insbesondere Daten, die im integralen Analysesystem (IASA NDB) bearbeitet werden, für eine sehr lange Dauer aufbewahrt werden dürfen; die Frist beträgt für Quellendokumente bis zu 45 Jahre, wobei, wie vorstehend erwogen, unklar bleibt, wie sich diese Dauer genau bestimmt (vgl. Art. 21 Abs. 1 Bst. b und d VIS-NDB). Nach der Rechtsprechung des EGMR kommt eine solche Frist in der Praxis einer unbefristeten Aufbewahrung gleich (vgl. zit. Urteil M.K., § 45 betreffend eine Frist von 25 Jahren). Gemäss Art. 20 VIS-NDB sind Personendatensätze durch die für die Erfassung zuständigen Mitarbeitenden periodisch unter anderem daraufhin zu überprüfen, ob sie weiterhin benötigt werden. Nicht mehr benötigte Daten sind zu löschen (vgl. Art. 20 Abs. 2 Bst. a und b VIS-NDB). Die periodische Überprüfung ist - je nach Themenbereich - nach Ablauf von 10, 15 oder 20 Jahren seit der Erfassung eines Objekts beziehungsweise seit der letzten periodischen Überprüfung vorzunehmen (Art. 20 Abs. 3 VIS-NDB; vgl. zur Qualitätssicherung auch vorstehend E. 16.2.2). Für unstrukturiert erfasste Originaldokumente schreibt Art. 11 Abs. 2 VIS-NDB lediglich eine jährliche stichprobenweise Überprüfung durch die Qualitätssicherungsstelle der Vorinstanz vor. Die Dauer der Bearbeitung von Resultaten aus der Kabelaufklärung kommt damit hier selbst unter Berücksichtigung der Vorgaben zur Qualitätskontrolle einer unbefristeten Aufbewahrung im Sinne der Rechtsprechung des EGMR zumindest sehr nahe. Die maximal zulässige Aufbewahrungsdauer beträgt zudem bis zu 45 Jahre, ohne dass hierfür eine besondere Rechtfertigung erforderlich wäre, die von einer unabhängigen Stelle überprüft würde. Das anwendbare Recht bietet damit in Bezug auf die Dauer der Aufbewahrung von Resultaten aus der Funk- und Kabelaufklärung weder einen ausreichend vorhersehbaren noch in der Sache hinreichenden Schutz vor Missbrauch. Ob dieser Mangel durch einen hinreichend effektiven nachträglichen Rechtsschutz ausgeglichen werden kann, wird im Rahmen der gesamthaften Beurteilung unter Berücksichtigung der Ergebnisse zu Prüfpunkt 8 zu beurteilen sein (vgl. nachfolgend E. 25). Das anwendbare Recht schreibt schliesslich nicht vor, dass die Daten nach Ablauf der zulässigen Aufbewahrungsdauer automatisch gelöscht werden müssen. Der Beigeladene hat jedoch nach eigenen Angaben seine Systeme so konfiguriert, dass die Daten, das heisst die erfassten Kommunikationen und die

Randdaten, spätestens nach Ablauf der Aufbewahrungsfristen automatisch gelöscht werden. Dasselbe gilt für die von der Vorinstanz im integralen Analysesystem (IASA NDB) bearbeiteten Daten. In den weiteren hier interessierenden Informationssystemen der Vorinstanz werden die Daten regelmässig auch in Bezug auf ihre Aufbewahrungsdauer hin überprüft und manuell gelöscht. Die Vorinstanz protokolliert zudem das Löschen und Vernichten von Daten und ermöglicht damit eine Überprüfung ihrer Tätigkeit im Rahmen der Aufsicht (vgl. zur Löschung und zur Protokollierung der Löschung einschliesslich der Aufbewahrung der Löschungsprotokolle den zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Ziffn. 169 und 200 ff.). Obschon hier weder eine Pflicht zur automatischen Löschung noch die Protokollierung gesetzlich vorgeschrieben sind und offen ist, ob der Beigeladene die Löschung der erfassten Inhalts- und Verbindungsdaten ebenfalls protokolliert, bietet die Praxis des Beigeladenen und der Vorinstanz ausreichend Schutz vor Missbrauch (vgl. zur fehlenden Pflicht zur Aussonderung und Löschung von Kommunikation im Zusammenhang mit dem Quellenschutz vorstehend E. 16.3.6.2).

E. 18.4

Zum sechsten Prüfpunkt ist zusammenfassend festzuhalten, dass das anwendbare Recht die Dauer einer Kabelaufklärung hinreichend vorhersehbar und in angemessener Weise begrenzt. Hingegen ist nicht hinreichend bestimmt vorgeschrieben, eine Kabelaufklärung fortlaufend auf ihre Erforderlichkeit hin zu überprüfen und diese vorzeitig zu beenden, sollte sich die Massnahme als nicht mehr erforderlich erweisen. Damit ist nicht gewährleistet, dass die Datenbearbeitung auf das notwendige Mass begrenzt ist. Dasselbe gilt in Bezug auf Aufträge zur Funkaufklärung, deren Dauer durch das anwendbare Recht nicht begrenzt ist. Was die Dauer der Aufbewahrung und die Pflicht zur Löschung von Daten betrifft, ist zwischen der Datenbearbeitung durch den Beigeladenen und die Vorinstanz zu unterscheiden. Für den Beigeladenen besteht diesbezüglich eine hinreichende gesetzliche Grundlage. Demgegenüber begrenzt das anwendbare Recht die Dauer der Aufbewahrung von Resultaten aus der Funk- und Kabelaufklärung durch die Vorinstanz nicht im erforderlichen Mass; es ist weder ausreichend vorhersehbar noch bietet es mit Blick auf die Dauer der zulässigen Aufbewahrung einen hinreichenden Schutz vor Missbrauch. Ob diese Mängel durch andere Garantien zum Schutz vor Missbrauch ausgeglichen werden können, ist im Rahmen der Gesamtbeurteilung unter Berücksichtigung insbesondere der Ergebnisse zu Prüfpunkt 8 zu beurteilen (vgl. hierzu nachfolgend E. 25). Prüfpunkt 7 die Verfahren und Modalitäten für die Kontrolle durch eine unabhängige Behörde im Hinblick auf die Einhaltung der Garantien und deren Befugnisse im Falle der Nichteinhaltung

E. 19.1

Für den EGMR ist von grundlegender Bedeutung, dass jede Phase der Massenüberwachung der Beaufsichtigung durch eine unabhängige Behörde unterworfen ist. Die Behörde muss zudem über ausreichend Befugnisse verfügen, um die Überwachung und damit die Beeinträchtigung des Privatbereichs und der Medienfreiheit auf das in einer demokratischen Gesellschaft notwendige zu beschränken. Insbesondere muss sie befugt und in der Lage sein, die Notwendigkeit und Verhältnismässigkeit der gesetzten Handlungen zu beurteilen (zit. Urteil Big Brother Watch und andere, § 356). Die für die Beaufsichtigung zuständige Behörde muss unabhängig sein. In Schweden und im Vereinigten Königreich bestand die Aufsichtsbehörde gemäss damals geltendem Recht aus (ehemaligen) Richterinnen und

Richtern, die von der Regierung (auf Vorschlag des Parlaments) für eine bestimmte Dauer ernannt wurden. Sie handelten unabhängig und verfügten über weitreichende Untersuchungsbefugnisse; konkret hatten sie etwa Zugang zu allen Unterlagen und durften Mitarbeitende befragen. In der Praxis untersuchten sie beispielsweise ausgewählte Überwachungsaufträge auf ihre Notwendigkeit und Verhältnismässigkeit hin, überprüften die Fälle, in denen schützenswerte beziehungsweise vertrauliche Kommunikation erfasst worden war, und nahmen eine Überprüfung der Verfahren für die Speicherung und Vernichtung der erfassten Kommunikationen vor (zit. Urteile Big Brother Watch und andere, §§ 135 ff. und 407 f. sowie Centrum för rättvisa, §§ 345-348). Im Vereinigten Königreich erstattete die zuständige Behörde, der «Interception of Communications Commissioner», der Regierung regelmässig Bericht. Zudem konnte er förmliche Empfehlungen aussprechen. Die Berichte der Behörde wurden jeweils vollständig veröffentlicht (zit. Urteil Big Brother Watch und andere, § 407). Die Aufsichtsbehörde in Schweden wiederum war befugt, verbindlich über die Beendigung einer Überwachungsmassnahme und über die Vernichtung von erfassten Daten zu entscheiden. Soweit die Aufsichtsbehörde grundsätzliche Empfehlungen aussprach, wurden diese ernsthaft geprüft (zit. Urteil Centrum för rättvisa, § 350). In beiden Ländern führten die Aufsichtsbehörden mehrere Inspektionen bei den für die Überwachung zuständigen Stellen durch. Im Vereinigten Königreich überprüfte die Behörde eine erhebliche Anzahl der Anordnungen zur Überwachung (zit. Urteile Big Brother Watch und andere, § 409 und Centrum för rättvisa, § 351). Der EGMR kam in beiden Verfahren zu dem Ergebnis, dass eine unabhängige und wirksame Aufsicht bestand, die in der Lage war, die Notwendigkeit und Verhältnismässigkeit einer beträchtlichen Anzahl von Überwachungsmassnahmen zu beurteilen (Urteile Big Brother Watch und andere, § 412 und Centrum för rättvisa, § 353). In seiner Entscheidung Centrum för rättvisa wies der Gerichtshof ausdrücklich auf das Zusammenspiel der verschiedenen Massnahmen zum Schutz vor Missbrauch hin (zit. Urteil Centrum för rättvisa, § 353): [...] De l'avis de la Cour, le rôle de l'Inspection, d'une part, et la procédure judiciaire d'autorisation préalable par le tribunal pour le renseignement extérieur, d'autre part, constituent ensemble une garantie efficace contre les abus aux stades essentiels du processus de ROEM [renseignement d'origine électromagnétique] : avant et pendant l'interception, l'analyse, l'utilisation et la destruction des informations obtenues.

E. 19.2

Das deutsche Bundesverfassungsgericht, das die Massenüberwachung - im deutschen Recht als strategische Telekommunikationsüberwachung bezeichnet - nach einem vergleichbaren Ansatz prüft, misst der Kontrolle ebenfalls eine grundlegende Bedeutung zu. Dabei fasst das Bundesverfassungsgericht die «unabhängige Rechtskontrolle administrativen Charakters» (hier Prüfpunkt 7) und die «gerichtsähnlich ausgestaltete Kontrolle» (hier Prüfpunkt 8) unter dem übergeordneten Erfordernis nach einer unabhängigen objektivrechtlichen Kontrolle zusammen und verlangt, dass im Zusammenwirken der Kontrollinstanzen der gesamte Prozess der Überwachung einer umfassenden Kontrolle unterliege. In diesem Sinne müsse eine Massenüberwachung, damit sie verhältnismässig ist, «durch eine effektive unabhängige objektivrechtliche Kontrolle flankiert» sein. Die Kontrolle sei kontinuierlich beziehungsweise fortlaufend und umfassend auszugestalten und auf die Wahrung der Grundrechte auszurichten (zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Rz. 170 und zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, Rz. 272 ff.). Zur Begründung dieser hohen Anforderungen hielt das deutsche

Bundesverfassungsgericht fest (zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Rz. 171): Die verfassungsrechtlichen Anforderungen an die Ausgestaltung der objektivrechtlichen Kontrolle der strategischen Überwachung sind besonders hoch. Denn mit der Kontrolle ist ein Ausgleich dafür zu schaffen, dass übliche rechtsstaatliche Sicherungen in weitem Umfang ausfallen. Zum einen muss die Kontrolle die faktische Schwäche der individuellen Rechtsschutzmöglichkeiten ausgleichen, die aus den nur begrenzten Auskunfts- und Benachrichtigungspflichten folgt. Zum anderen hat sie die im Wesentlichen nur finale Anleitung der Überwachungsbefugnisse zu kompensieren. [...] Sie bildet damit ein notwendiges Gegengewicht zu den weiten Handlungsmöglichkeiten des Bundesnachrichtendienstes [...].

E. 20.1

Die Kontrolle und Aufsicht über die Tätigkeit des Beigeladenen und der Vorinstanz ist in den Art. 75 ff. NDG geregelt. Demnach stellt die Vorinstanz zunächst und in erster Linie selbst durch geeignete Qualitätssicherungs- und Kontrollmassnahmen sicher, dass der rechtskonforme Vollzug des Gesetzes gewährleistet ist (Art. 75 NDG; vgl. auch Botschaft NDG, BBl 2014 2105, 2201). Aufsichtsstellen sind die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND (Art. 76 f. NDG) und die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI (Art. 79 NDG). Die parlamentarische Oberaufsicht obliegt der Geschäftsprüfungsdelegation GPDel (Art. 81 Abs. 1 NDG). Im Folgenden ist getrennt auf die Stellung, die Aufgaben und die Befugnisse der zwei Aufsichtsstellen und der parlamentarischen Oberaufsicht einzugehen. Zudem ist jeweils die Anwendungspraxis darzustellen.

E. 20.2.1

Gemäss Art. 76 Abs. 1 NDG schafft der Bundesrat eine unabhängige Behörde zur Aufsicht über die Vorinstanz. Der Leiter der Aufsichtsbehörde wird für eine Amtsdauer von sechs Jahren vom Bundesrat gewählt (Art. 76 Abs. 2 NDG). Die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND übt ihre Funktion unabhängig aus; sie ist nicht weisungsgebunden. Administrativ ist sie dem Departement für Verteidigung, Bevölkerungsschutz und Sport VBS zugeordnet (Art. 77 Abs. 1 NDG). Die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND beaufsichtigt die nachrichtendienstliche Tätigkeit der Vorinstanz und überprüft deren Tätigkeit auf Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit (Art. 78 Abs. 1 NDG). Sie koordiniert ihre Tätigkeit mit den anderen Aufsichtsstellen (Art. 78 Abs. 2 NDG). Für ihre Tätigkeit hat die Aufsichtsbehörde Zugang zu allen sachdienlichen Informationen und Unterlagen einschliesslich der Informationssysteme und Datenbanken sowie Zutritt zu allen Räumlichkeiten der beaufsichtigten Stellen (Art. 78 Abs. 4 und 5 NDG). Sie kann zudem Befragungen durchführen und die Mitarbeitenden sind verpflichtet, vollständig und wahrheitsgetreu Auskunft zu erteilen (Art. 6 Abs. 1 VAND). Das Ergebnis ihrer Überprüfungen teilt die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND dem Departement schriftlich mit. Sie kann Empfehlungen aussprechen (Art. 78 Abs. 6 NDG). Das Departement sorgt für die Umsetzung der Empfehlungen. Weist es eine Empfehlung zurück, unterbreitet es diese dem Bundesrat zum Entscheid (Art. 78 Abs. 7 NDG). Zusätzlich informiert die Aufsichtsbehörde über ihre Tätigkeit in einem jährlichen Bericht, der veröffentlicht wird (Art. 78 Abs. 3 NDG; vgl. für die Tätigkeitsberichte < www.ab-nd.admin.ch > Tätigkeitsberichte, abgerufen am 16. Oktober 2025).

E. 20.2.2

Die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND äussert sich in ihren Stellungnahmen vom 11. Oktober 2022 und vom 8. April 2025 zunächst zu ihrer Zuständigkeit und zur Koordination ihrer Tätigkeit mit derjenigen der anderen Aufsichtsbehörden. Demnach obliegt die Beurteilung der Rechtmässigkeit der Informationsbeschaffung durch den Beigeladenen der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI (hierzu nachfolgend E. 20.3); die Rechtmässigkeit der Informationsbeschaffung werde von der Aufsichtsbehörde nicht zusätzlich zur Kontrollinstanz überprüft. Sie sei jedoch im Austausch mit der Kontrollinstanz und nehme insbesondere an deren Inspektionen teil. Die Aufsichtsbehörde sei ihrerseits zuständig für die Überprüfung beziehungsweise Kontrolle der Rechtmässigkeit der an die Beschaffung anschliessenden Bearbeitung von Daten aus der Funk- und Kabelaufklärung durch die Vorinstanz. Die Prüfungstätigkeit der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND erfolge sodann «risikoorientiert» auf der Grundlage eines jährlichen Prüfungsplans. Gemäss der Stellungnahme vom 8. April 2025 hat die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND bisher nicht explizit geprüft, ob die Bearbeitung von Daten aus der Kabelaufklärung durch die Vorinstanz rechtmässig erfolgt. Die Aufsichtsbehörde prüfe die Datenablage und Datenbearbeitung der Vorinstanz vielmehr in genereller Weise, «sofern Risiken vorhanden» seien. Entsprechend sei in verschiedenen Informationssystemen die Rechtmässigkeit der Datenbearbeitung einer Überprüfung unterzogen worden, wobei hierbei die Einhaltung der Datenbearbeitungsschranken, Protokollierungspflichten und Aufbewahrungsfristen im Mittelpunkt gestanden hätten, nicht jedoch die Herkunft der Daten. Im Rahmen ihrer Tätigkeit habe festgestellt werden können, dass die Vorinstanz nicht systematisch gegen die gesetzlich festgelegten Bearbeitungsschranken und die weiteren Vorgaben zur Datenbearbeitung verstosse.

E. 20.3.1

Gemäss Art. 79 Abs. 1 NDG prüft die verwaltungsinterne unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung (UKI) die Funkaufklärung auf Rechtmässigkeit und beaufsichtigt den Vollzug der genehmigten und freigegebenen Aufträge zur Kabelaufklärung. Sie versieht ihre Aufgaben weisungsungebunden. Ihre Mitglieder werden vom Bundesrat für eine Amtsdauer von vier Jahren gewählt (Art. 79 Abs. 4 Satz 2 NDG). Die Kontrollinstanz prüft die Aufträge an den Beigeladenen als dem durchführenden Dienst sowie die Bearbeitung und Weiterleitung der Informationen, die dieser erfasst hat. Sie erhält dazu von den zuständigen Stellen Zugang zu allen zweckdienlichen Informationen und Anlagen (Art. 79 Abs. 2 NDG). Sie kann aufgrund der Überprüfung Empfehlungen abgeben und beim Departement für Verteidigung, Bevölkerungsschutz und Sport VBS beantragen, dass Aufträge zur Funkaufklärung eingestellt und Informationen gelöscht werden. Ihre Empfehlungen, Anträge und Berichte sind nicht öffentlich (Art. 79 Abs. 3 NDG). Die Organisation und die Aufgaben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI sind in der VAND geregelt beziehungsweise konkretisiert (Art. 1 Bst. b VAND). Demnach setzt sich die Kontrollinstanz aus drei bis fünf Angehörigen der Bundesverwaltung zusammen, wobei die Mitglieder über Fachkenntnisse in den Bereichen Telekommunikation, Sicherheitspolitik und Grundrechtsschutz verfügen müssen (Art. 7 Abs. 1 und 2 VAND; vgl. auch Art. 7 Abs. 3 VAND). Im Rahmen ihres Kontrollauftrags überprüft die Kontrollinstanz gemäss Art. 10 Abs. 1 VAND die Funkaufklärungsaufträge

auf ihre Rechtmässigkeit (Bst. a), sie sieht die Aufträge zur Kabelaufklärung einschliesslich der Genehmigungsentscheide und der Freigaben ein (Bst. b) und untersucht die Resultate der Funk- und Kabelaufklärung (mittlerweile) stichprobenweise (Bst. d). Sie sieht zudem die Dokumente des Beigeladenen zu Planung, Ablauf und Nutzen der Funk- und Kabelaufklärungsaufträge ein und untersucht die Abläufe, Daten und Systeme des Beigeladenen (Bst. c und e). Hierzu kann sie Mitarbeitende der Vorinstanz und des Beigeladenen befragen (Bst. f). Gemäss Art. 10 Abs. 2 VAND prüft die Kontrollinstanz die Funkaufklärungsaufträge in der Regel jährlich und den Vollzug der Kabelaufklärungsaufträge innerhalb von sechs Monaten ab Beginn der Aufklärung beziehungsweise jährlich, wenn die Ausführung länger als sechs Monate dauert. Sie erstattet dem Bundesrat jährlich Bericht über ihre Prüfungen. Bereits aus dem Gesetzesmaterialien ergibt sich, dass die Kontrollinstanz nicht umfassend kontrollieren, sondern mit «geeigneten Überprüfungen» sicherstellen soll, dass der Beigeladene und die Vorinstanz die gesetzlichen Vorschriften einhalten (Botschaft NDG, BBl 2014 2105, 2203).

E. 20.3.2

Die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI äussert sich im Rahmen ihrer Antworten zu den Fragenkatalogen des Bundesverwaltungsgerichts zu ihrer Aufsichtstätigkeit. Demnach prüft die Kontrollinstanz mindestens einmal jährlich alle Aufträge zur Funkaufklärung auf ihre Rechtmässigkeit hin. Im Vordergrund hierbei stehe die Überprüfung der Suchbegriffe und die Überprüfung der konkreten Resultate aus der Funkaufklärung auf ihre Rechtmässigkeit hin, einschliesslich deren Verwendung durch die Vorinstanz (Stellungnahme der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 5. Oktober 2022, Beilage, S. 2). Die Kontrollinstanz beaufsichtige sodann den Vollzug von genehmigten und freigegebenen Aufträgen zur Kabelaufklärung. Hierzu führe sie jährlich vier Inspektionen bei der Vorinstanz und einen Kontrollbesuch beim Beigeladenen durch. Im Zentrum der Aufsichtstätigkeit stehe die Rechtmässigkeit der Datenbeschaffung durch den Beigeladenen, das Generieren von Produkten und das Weiterleiten von diesen an die Vorinstanz. Hierzu werde der gesamte Bearbeitungsprozess von der Verwendung eines einzelnen Suchbegriffs bis zum daraus resultierenden Aufklärungsresultat überprüft. Die hierfür erforderlichen Unterlagen würden der Kontrollinstanz jeweils vor Ort vorgelegt. Die Rechtmässigkeit eines Auftrags zur Kabelaufklärung an sich werde nicht überprüft; dies sei Sache des Bundesverwaltungsgerichts im Rahmen des Genehmigungsverfahrens. Ebenfalls nicht in ihre Zuständigkeit falle die Beaufsichtigung der Datenbearbeitung durch die Vorinstanz; dies sei Sache der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND (Stellungnahme der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 26. Oktober 2023; Stellungnahme der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 5. Oktober 2022, Beilage, S. 1 und S. 5). Für die Beurteilung der Rechtmässigkeit von Aufklärungsprodukten aus der Kabelaufklärung stützt sich die Kontrollinstanz auf die Genehmigung des Bundesverwaltungsgerichts und den Freigabeentscheid des Departements. Diese erhalte sie jeweils direkt zugestellt. Es werde insbesondere überprüft, ob ein hinreichender Aufgabenbezug (Art. 6 NDG) gegeben sei, ob sich der dem Resultat zu Grunde liegenden Suchbegriff einer bewilligten Kategorie von Suchbegriffen zuordnen lasse und ob das Resultat keinen unzulässigen Bezug zum Inland aufweise. Die Kontrolle erfolge stichprobenweise anhand von 20 Resultaten «pro Untersuchungszeitraum». Ein besonderes Augenmerk lege die Kontrollinstanz auf Aufklärungsaufträge und -produkte, die einen

Bezug zur Schweiz aufweisen würden (Stellungnahem der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 5. Oktober 2022, Beilage, S. 1 und 3). Die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI hält schliesslich fest, es sei nicht ihre Aufgabe, den Beigeladenen systematisch zu kontrollieren. Ziel der Kontrollbesuche sei es vielmehr, ein möglichst vollständiges Bild von der Funk- und Kabelaufklärung zu erhalten; es gehe dabei um Fragen, wie Signale ausgeleitet und erfasst, wie Produkte für die Vorinstanz erstellt und wie Suchbegriffe in den Systemen konfiguriert würden. In Kenntnis dessen überprüfe die Kontrollinstanz jeweils auch, wie der Beigeladene die Aufträge der Vorinstanz bearbeite. Als Milizgremium sei sie jedoch nicht in der Lage, die Systeme des Beigeladenen beziehungsweise deren Nutzung systematisch zu kontrollieren. Zudem sei die Kontrollinstanz organisatorisch und ressourcenmässig «bescheiden ausgestattet». Ihre Aufgabe sei es in diesem Sinne, den «übergeordneten» Kontrollinstanzen, der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND und der Geschäftsprüfungsdelegation GPDel, sachbereichsspezifische Unterstützung zu bieten. Eine quantitativ und qualitativ tiefgreifendere Prüfung der Tätigkeiten von Vorinstanz und Beigeladenem sei nicht möglich (Stellungnahme der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 26. Oktober 2023; Stellungnahme der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 5. Oktober 2022, Beilage, S. 5, 6 und 7). Gemäss Art. 10 Abs. 3 VAND erstattet die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI dem Departement für Verteidigung, Bevölkerungsschutz und Sport VBS jährlich Bericht über ihre Prüfungen. Sie kann darin Empfehlungen aussprechen. Die Kontrollinstanz edierte dem Bundesverwaltungsgericht die Berichte für die Jahre 2019 - 2024 im Original. Mit Schreiben vom 25. August 2025 reichte die Kontrollinstanz dem Bundesverwaltungsgericht die Berichte zudem in teilweise geschwärzter Form ein. Sie begründet die Schwärzungen im Wesentlichen damit, dass die betreffenden Passagen konkrete Angaben zur Beschaffung von Informationen im Ausland durch die Vorinstanz enthielten beziehungsweise Rückschlüsse darauf zuliessen und daher geheim zu halten seien (Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung vom 25. August 2025, beiliegende Aktennotiz vom 22. August 2025; vgl. zudem vorstehend E. 7.6.3). Die Jahresberichte bestätigen zunächst die parteiöffentlichen Ausführungen der Kontrollinstanz in Bezug auf Umfang und Schwerpunkt ihrer Aufsichtstätigkeit. Sie überprüft demnach insbesondere die Rechtmässigkeit von Resultaten aus der Funkaufklärung. Die Überprüfung erfolgt anhand von Stichproben zufällig ausgewählter Resultate während der vier im Jahr stattfindenden Inspektionen, wobei die Vorinstanz die für eine Überprüfung erforderlichen Kontextinformationen zur Verfügung stellt. Die Überprüfung erfolgt hinsichtlich Rechtmässigkeit und damit verbunden hinsichtlich Plausibilität und Nachvollziehbarkeit. Mit in die Kontrolle einbezogen werden auch die Suchbegriffe (sog. Targetlisten). Schliesslich kontrolliert die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI die Aufträge und Resultate mit einem sogenannten Schweiz-Bezug (unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI, Jahresbericht 2019 - 2024, im Original zu den Akten genommen mit Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 5. Oktober 2022, 7. September 2023 und 30. Juli 2025 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 9. September 2025]) Gemäss den Jahresberichten nimmt die Kontrollinstanz ihre Prüfungen auch in Bezug auf die Kabelaufklärung mittels Stichproben vor; Grundlage sei eine Liste mit allen durch Kabelaufklärung erzielten

Aufklärungsprodukten, die der Kontrollinstanz jeweils vorgelegt werde. Die zu kontrollierenden Produkte würden zufällig ausgewählt (vgl. Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung vom 25 August 2025, beiliegender teilweise geschwärzter Jahresbericht 2024, S. 4; zudem die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI, Jahresberichte 2019 - 2023, im Original zu den Akten genommen mit Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung vom 5. Oktober 2022, 7. September 2023 und 30. Juli 2025 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 9. September 2025]). Für die Überprüfung erhalte die Kontrollinstanz sodann Kontextinformationen, um die Rechtmässigkeit der Resultate beurteilen zu können. Überprüft werde insbesondere, ob es sich beim konkret verwendeten Suchbegriff um einen zulässigen Suchbegriff handle und ob die Schranken gemäss Art. 39 Abs. 2 und 3 NDG beachtet worden seien. Hierzu lasse sich die Kontrollinstanz vom Beigeladenen jeweils zeigen, wie rein inländische Kommunikation identifiziert und ausgesondert werde. Zudem werde kontrolliert, ob der Beigeladene erfasste Daten nicht länger als zulässig aufbewahre und anschliessend lösche. In den Jahresberichten findet sich weiter die Feststellung, dass die Kategorien von Suchbegriffen so weit formuliert seien, dass diesen kaum die vom Gesetzgeber gewünschte begrenzende Filter- und Schutzfunktion zukomme. Die Kontrollinstanz beurteile die Zulässigkeit der verwendeten Suchbegriffe daher insbesondere auch anhand der Genehmigungsverfügung und damit anhand der Orientierung und des Bedürfnisses (vgl. hierzu vorstehend E. 14.2.1), wobei nicht immer einfach überprüft werden könne, ob die Suchbegriffe im Sinne von Art. 39 Abs. 3 NDG so gewählt seien, dass ihre Anwendung möglichst geringe Eingriffe in das Privatleben von Personen verursacht. Schliesslich ergibt sich aus den Jahresberichten, dass sich die Kontrollinstanz jeweils alle Anträge um Entanonymisierung von Informationen über Personen in der Schweiz in Resultaten aus der Funk- und Kabelaufklärung vorlegen lässt und anhand von Kontextinformationen deren Nachvollziehbarkeit und Rechtmässigkeit prüft. Die Kontrollinstanz äussert sich in ihren Berichten aus jeweils aktuellem Anlass sodann auch zu konkreten Fragestellungen im Zusammenhang mit der Kabelaufklärung. Insgesamt bestand für die Kontrollinstanz in den letzten Jahren kein Anlass, förmliche Empfehlungen auszusprechen; die anlässlich der Inspektionen und von Gesprächen angeregten Änderungen seien bisher stets umgesetzt worden (vgl. Stellungnahmen der der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung [UKI] vom 5. Oktober 2022, S. 1 und 4 f.; unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI, Jahresbericht 2019 - 2024, im Original zu den Akten genommen mit Schreiben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI vom 5. Oktober 2022, 7. September 2023 und 30. Juli 2025 [wesentlicher Inhalt bekannt gegeben mit Zwischenverfügung vom 9. September 2025]).

E. 20.4.1

Die parlamentarische Oberaufsicht über die Tätigkeit der Vorinstanz obliegt in ihren jeweiligen Zuständigkeitsbereichen der Geschäftsprüfungsdelegation GPDel und der Finanzdelegation nach Massgabe des Parlamentsgesetzes (ParlG, SR 171.10; Art. 81 Abs. 1 NDG). Gemäss Art. 53 Abs. 2 ParlG überwacht die Geschäftsprüfungsdelegation GPDel die Tätigkeit im Bereich des Staatsschutzes und der Nachrichtendienste und überprüft das staatliche Handeln in Bereichen, die geheim gehalten werden, weil deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen schweren Schaden zufügen kann. Zur Erfüllung ihrer Aufgaben hat die Delegation Zugang zu allen sachdienlichen Unterlagen; sie hat insbesondere das Recht auf Herausgabe von Unterlagen, die im Interesse des

Staatsschutzes oder der Nachrichtendienste als geheim klassifiziert sind oder deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen schweren Schaden zufügen kann (Art. 154 Abs. 2 Bst. a Ziff. 2 ParlG). In ihrer Stellungnahme vom 28. Oktober 2022 zum Fragenkatalog des Bundesverwaltungsgerichts führte die Geschäftsprüfungsdelegation GPDel aus, sie erhalte zum Zweck ihrer Oberaufsicht über die nachrichtendienstlichen Tätigkeiten insbesondere die jährlichen Leistungsausweise zur Kommunikationsüberwachung, die Tätigkeitsberichte des Bundesverwaltungsgerichts (Abteilung I, Fachgebiet NDG) und die Jahresberichte der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI. Zudem führe sie zumindest ein Mal im Jahr einen «Dienststellenbesuch» beim Beigeladenen durch, um sich über Entwicklung, Herausforderungen und Praxis der Funk- und Kabelaufklärung zu informieren. Dabei ginge es um das Funktionieren des Gesamtsystems; eine inhaltliche Kontrolle konkreter Entscheide im Rahmen der Oberaufsicht sei ausgeschlossen. Stosse die Geschäftsprüfungsdelegation GPDel auf Sachverhalte, die grundlegende Probleme oder Fragen in ihrem Kompetenzbereich betreffen würden, greife sie zum Mittel der formellen Untersuchung. Diese führe in der Regel dazu, dass die Delegation Empfehlungen an die betroffene Behörde richte. Empfehlungen seien zwar nicht verbindlich, die verantwortliche Behörde sei jedoch verpflichtet, Abweichungen von der Einschätzung der Delegation zu begründen. Eine solche Untersuchung sei im Jahr 2019 auch bei der Vorinstanz durchgeführt worden. Dabei habe die Geschäftsprüfungsdelegation GPDel feststellen müssen, dass die Vorinstanz die Bearbeitungsschranke gemäss Art. 5 Abs. 5 NDG nicht hinreichend beachtet. Bis zum Zeitpunkt der Stellungnahme im Rahmen des vorliegenden Beschwerdeverfahrens habe die Geschäftsprüfungsdelegation GPDel keine Gewähr, dass die Vorinstanz und der Beigeladene Daten rechtmässig unter Einhaltung der Datenbearbeitungsschranke bearbeiten. Verbesserungspotential sieht die Geschäftsprüfungsdelegation GPDel auch bei der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND; diese reagiere zu zögerlich.

E. 21.1

Die Beurteilung des Verfahrens und der Modalitäten für die Aufsicht durch eine unabhängige Behörde im Hinblick auf die Einhaltung der Vorgaben für die Funk- und Kabelaufklärung und deren Befugnisse im Falle der Nichteinhaltung ist gemäss der Rechtsprechung der Grossen Kammer des EGMR auf folgende Kriterien abzustützen: - Unabhängigkeit der Aufsichtsbehörde - Umfang der Aufsichtstätigkeit - Befugnisse der Aufsichtsbehörde

E. 21.2.1

Der EGMR fokussiert im Rahmen des siebten Prüfpunktes auf die Überwachung der Informationsbeschaffung. Diese Aufgabe kommt nach Schweizer Recht der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI zu. Deren Tätigkeit steht daher hier im Vordergrund (nachfolgend E. 21.2.2). Aufgrund der dem Schweizer Recht eigenen Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung und der Bedeutung auch der Datenbearbeitung durch die Vorinstanz ist hiernach zusätzlich auf die Tätigkeit der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND einzugehen (nachfolgend E. 21.2.3).

E. 21.2.2

Die Unabhängigkeit der Kontrollinstanz ist in Art. 79 Abs. 1 NDG gesetzlich verankert. Zudem besteht mit Blick auf die gesetzlichen Vorgaben zu Wahl, Zusammensetzung und Organisation sowie angesichts von deren tatsächlicher Aufsichtstätigkeit kein begründeterer Anlass für die Annahme, die Kontrollinstanz würde ihre Aufgabe nicht unabhängig wahrnehmen. Die Kontrollinstanz überprüft die Funkaufklärungsaufträge auf ihre Rechtmässigkeit hin und beaufsichtigt den Vollzug der genehmigten und freigegebenen Aufträge zur Kabelüberwachung. In Bezug auf die Kabelaufklärung überwacht sie den gesamten Bearbeitungsprozess von der Verwendung eines einzelnen Suchbegriffs bis zum daraus resultierenden Aufklärungsresultat und deren Weiterleiten an die Vorinstanz. Die Kontrollinstanz hat im Rahmen ihrer Tätigkeiten gemäss Art. 10 VAND Zugang zu allen zweckdienlichen Informationen und Anlagen. Sie überwacht die Tätigkeit des Beigeladenen insofern grundsätzlich umfassend mit dem Ziel, die Rechtmässigkeit der Datenbearbeitung durch den Beigeladenen zu gewährleisten. Daran ändert für sich alleine schliesslich nichts, dass die Kontrollinstanz nicht selbst unmittelbar Zugriff auf die Systeme und die Datenablage des Beigeladenen hat; ein solcher Zugriff wäre wiederum selbst mit einem nicht unerheblichen Missbrauchspotential verbunden. Näher einzugehen ist im Folgenden auf den Umfang der Aufsichtstätigkeit und die Befugnisse der Kontrollinstanz. Gemäss dem vorstehend insbesondere auch zur tatsächlichen Aufsichtstätigkeit Dargelegten führt die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI im Jahr vier Inspektionen bei der Vorinstanz und einen Kontrollbesuch beim Beigeladenen durch. Während der Inspektionen überprüft sie stichprobenweise - im Rahmen der Kabelaufklärung erfolgt die Überprüfung anhand von 20 Resultaten «pro Untersuchungszeitraum» - die Rechtmässigkeit von Resultaten aus der Funk- und Kabelaufklärung. Ein Schwerpunkt der Aufsichtstätigkeit sind sodann die Anträge auf Entanonymisierung und die Resultate mit einem Schweiz-Bezug; gemäss den Berichten der Kontrollinstanz über ihre Prüfungen lässt sie sich alle Resultate mit einem Bezug zur Schweiz und die Anträge auf Entanonymisierung vorlegen, was sowohl zweckmässig als auch notwendig erscheint (vgl. hierzu auch vorstehend E. 9.4 und 16.3.4.3). Eine fortlaufende und effektive Beaufsichtigung der Informationsbeschaffung durch den Beigeladenen ist innerhalb dieses Rahmens insbesondere in quantitativer Hinsicht jedoch nicht gewährleistet (vgl. zit. Urteil Centrum för rättvisa, § 351; zudem BGE 149 I 218 E. 8.7.3). Die Aufsicht beschränkt sich in zeitlicher Hinsicht vielmehr auf fünf Kontrollen beziehungsweise Inspektionen im Jahr. Die Kontrollinstanz ist zudem auch nach eigenen Angaben nicht in der Lage, eine bedeutende Anzahl von Resultaten aus der Funk- und Kabelaufklärung auf ihre Rechtmässigkeit hin zu überprüfen. Weiter fällt in Betracht, dass die Tätigkeit der Kontrollinstanz im geheimen erfolgt; die Berichte der Kontrollinstanz über ihre Prüfungen werden nicht veröffentlich, wobei, wie das vorliegende Verfahren gezeigt hat, eine Veröffentlichung in geeigneter Form, das heisst mit Schwärzungen oder in Form einer Zusammenfassung, möglich wäre (vgl. zit. Urteil Big Brother Watch und andere, § 407). Die - grundsätzlich notwendige - Geheimhaltung der Überwachung selbst wird daher hier nicht durch eine geeignete Öffentlichkeit der Tätigkeit der Kontrollinstanz zumindest teilweise kompensiert. Die Kontrollinstanz hat sodann die Funkaufklärung gemäss Art. 10 Abs. 1 Bst. a VAND umfassend auf ihre Rechtmässigkeit hin zu überprüfen, wobei sie sich bei ihrer Tätigkeit nicht allein auf Überprüfung der Aufträge beschränkt, sondern in ihre Prüfungen auch die Suchbegriffe und konkrete Resultate einbezieht. Anders als in Bezug auf die Kabelaufklärung ergeben sich hinsichtlich der Funkaufklärung aus dem anwendbaren Recht - abgesehen vom erforderlichen Bezug der Funkaufklärung zum

Aufgabenbereich der Vorinstanz - keine Vorgaben in Bezug auf die Zulässigkeit der Funkaufklärung und es sind auch keine Einschränkungen in Bezug auf die Erfassung bestimmter Kommunikationen und die Verwendung von Suchbegriffen vorgesehen. Damit ist aber auch nicht ohne Weiteres nachvollziehbar, anhand welcher verbindlichen Vorgaben die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI die Rechtmässigkeit der Funkaufklärung überprüft. Schliesslich ist zu berücksichtigen, dass die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI nicht über die Befugnis verfügt, die Einstellung einer Überwachung oder das Löschen von Daten verbindlich anzuordnen, auch wenn dies nicht besonders stark ins Gewicht fällt, da in der Praxis Meinungsäusserungen der Kontrollinstanz berücksichtigt werden. Die Aufsicht durch die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI im Bereich der Informationsbeschaffung bietet nach dem Gesagten keinen fortlaufenden und effektiven und damit keinen hinreichenden Schutz vor Missbrauch. Dieser Mangel im Verfahren kann hier auch nicht durch die Aufsichtstätigkeit der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND und jene der parlamentarischen Oberaufsicht ausgeglichen werden; die Aufsichtsbehörde beaufsichtigt die Informationsbeschaffung durch den Beigeladenen ausdrücklich nicht und auch die Oberaufsicht nimmt keine inhaltliche Kontrolle einzelner Entscheide vor.

E. 21.2.3

Die Kontrolle über die Datenbearbeitung durch die Vorinstanz obliegt der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND. Die Aufsichtsbehörde ist unabhängig und die Unabhängigkeit ist in ausreichendem Mass institutionell und organisatorisch abgesichert; sie handelt weisungsungebunden, ihr Leiter wird vom Bundesrat gewählt, sie verfügt über ihr eigenes Budget und stellt ihr eigenes Personal an. Der Aufsichtsbehörde stehen zur Erfüllung ihrer Aufgaben umfassende Befugnisse zu. Sie ist jedoch nicht berechtigt, im Einzelfall das Löschen oder Berichtigen etwa von unrechtmässig und unrichtig bearbeiteten Daten verbindlich anzuordnen; sie kann nur - aber immerhin - Empfehlungen aussprechen. Zudem ist die Aufsichtsbehörde UKI - anders als die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung - nicht themenspezifisch zuständig, sondern Aufsichtsbehörde über die gesamten nachrichtendienstlichen Tätigkeiten und damit über einen weiten Bereich. Die Aufsicht über die Datenbearbeitung und Archivierung, die hier im Vordergrund steht, stellt denn auch einen Aufsichtsbereich unter vielen dar. Die Aufsichtstätigkeit erfolgt (aus diesem Grund) risikoorientiert. So kontrollierte die Aufsichtsbehörde im Bereich Datenbearbeitung und Archivierung in der jüngeren Vergangenheit etwa die Datenbearbeitung im Informationssystem Quattro P, in welchem die von den Grenzkontrollorganen übermittelten Daten bearbeitet werden, und im Informationssystem OSINT-Portal, das aus einer nach Quellen und Thematiken geordneten Datenablage zur Abfrage und Auswertung von Daten aus öffentlich zugänglichen Quellen besteht. Die Kontrolle erfolgte stichprobenweise anhand ausgewählter Beschaffungen. Die Tätigkeit der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND ist nach dem Gesagten und soweit aus den Stellungnahmen und aus den Jahresberichten ersichtlich, insgesamt auf das Erkennen systematischer Probleme etwa bei der Datenbearbeitung ausgerichtet. Dasselbe gilt auch für die Aufsicht durch Geschäftsprüfungsdelegation GPDel. Auch die Tätigkeit der unabhängigen Aufsichtsbehörde bietet mithin keine fortlaufende und effektive Beaufsichtigung der Bearbeitung von Daten (aus Resultaten der Funk- und Kabelaufklärung) durch die Vorinstanz. Ob dieser Mangel etwa durch eine effektive interne

Qualitätssicherung (vgl. hierzu Prüfpunkt 4) ausgeglichen werden kann, wird im Rahmen der Gesamtbeurteilung zu beurteilen sein (vgl. nachfolgend E. 25).

E. 21.3

Mit der laufenden Revision des Nachrichtendienstgesetzes sollen die Aufgaben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI an die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND übertragen werden. In den erläuternden Bericht zur Vernehmlassungsvorlage wird diesbezüglich ausgeführt, die Aufsichtsbehörde verfüge bereits über umfassende Aufsichtskompetenzen und habe Zugang zu allen sachdienlichen Informationen und Unterlagen. Die Kompetenzen der Aufsichtsbehörde würden grundsätzlich auch jene der Kontrollinstanz abdecken. Daher sei es sinnvoll, die Aufsichtstätigkeiten der beiden unabhängigen Stellen in einer einzigen Behörde zusammenzuführen. Die Aufsichtsbehörde verfüge zudem über die breitere Übersicht über die nachrichtendienstlichen Tätigkeiten. Mit der Übertragung der Aufgaben von der Kontrollinstanz an die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND werde eine umfassendere Aufsicht garantiert, die sich nicht nur auf die Rechtmässigkeit der nachrichtendienstlichen Tätigkeiten, sondern auch auf deren Zweckmässigkeit und Wirksamkeit erstrecke (Art. 78 Abs. 1 NDG im Vergleich zu Art. 79 Abs. 1 NDG). Insgesamt könnten Synergien genutzt werden, zumal es für die im Milizsystem arbeitende unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI zunehmend schwierig werde, auf dem nötigen Wissensstand zu bleiben, während die Aufsichtsbehörde bereits heute über Fachleute verfüge (vgl. Erläuternder Bericht Revision NDG, S. 30 f.). Der EGMR verlangt in seiner Rechtsprechung zur Massenüberwachung als Massnahme zum Schutz vor Missbrauch eine fortlaufende und effektive Kontrolle durch eine unabhängige Behörde. Eine solche Kontrolle ist alleine durch die Überführung der Aufgaben der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI an die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND nicht gewährleistet. Die Tätigkeit der Aufsichtsbehörde ist beziehungsweise wird im Rahmen der laufenden Revision gesetzlich nicht weiter - im Sinne der Anforderungen gemäss der Rechtsprechung des EGMR - konkretisiert und hängt damit - wie bisher - auch und im Wesentlichen von der personellen beziehungsweise finanziellen Ausstattung der Aufsichtsbehörde ab. Zudem ist (auch weiterhin) keine fortlaufende und in hinreichendem Mass effektive Kontrolle anhand einer bedeutenden Anzahl konkreter Resultate aus der Funk- und Kabelaufklärung vorgeschrieben.

E. 21.4

Zusammenfassend ist zum siebten Prüfpunkt festzuhalten, dass mit der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI eine unabhängige Behörde besteht, die den Vollzug der Aufträge zur Kabelüberwachung beaufsichtigt und zudem die Aufträge zur Funkaufklärung auf ihre Rechtmässigkeit hin überprüft. Das anwendbare Recht und die effektive Anwendungspraxis ermöglichen jedoch keine fortlaufende und effektive Beaufsichtigung der Informationsbeschaffung durch den Beigeladenen. Die Kontrollinstanz ist nicht in der Lage, eine bedeutende Anzahl an Resultaten auf ihre Rechtmässigkeit hin zu überprüfen und ihre Tätigkeit beschränkt sich auf fünf Kontrollen beziehungsweise Inspektionen im Jahrs. Eine fortlaufende und effektive Beaufsichtigung besteht auch nicht in Bezug auf die Datenbearbeitung durch die Vorinstanz; die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND prüft die

Datenbearbeitung risikoorientiert und stichprobenweise auf der Grundlage ausgewählter Beschaffungen. Beiden Behörden kommt sodann nicht die Befugnis zu, die Einstellung einer Überwachung oder das Löschen von Daten verbindlich anzuordnen. Insgesamt besteht daher in Bezug auf die Kontrolle durch eine unabhängige Behörde im Hinblick auf die Einhaltung der Garantien kein hinreichender Schutz vor Missbrauch. Dies fällt hier besonders ins Gewicht, da im Rahmen einer geheimen Massenüberwachung die üblichen rechtsstaatlichen Sicherungen in weitem Umfang ausfallen. Prüfpunkt 8 Das Verfahren für eine unabhängige nachträgliche Überprüfung der Einhaltung der Garantien und die Befugnisse des zuständigen Organs für den Fall der Nichteinhaltung

E. 22.1

Der EGMR misst schliesslich der unabhängigen nachträglichen Überprüfung grundlegende Bedeutung bei: Jedem, der Verdacht schöpft, dass seine Kommunikation nachrichtendienstlich überwacht wird, muss demnach ein wirksamer Rechtsbehelf zur Verfügung stehen, um entweder die Rechtmässigkeit der vermuteten Überwachung oder die Koventionskonformität des Überwachungsregimes an sich in Frage zu stellen. Der EGMR weist zudem darauf hin, dass die Wirksamkeit des Rechtsbehelfs im Rahmen der Massenüberwachung nicht davon abhängig ist, ob eine Benachrichtigung des Betroffenen über die Datenbearbeitung erfolgt; sieht das anwendbare Recht keine (hinreichende) Benachrichtigung vor, reicht es aus, wenn der Rechtsbehelf grundsätzlicher jedermann offen steht. Der Rechtsbehelf hat insgesamt hinreichend wirksam zu sein, wobei hinreichend im konkreten Kontext zu verstehen ist und meint, dass der Rechtsbehelf nur so wirksam sein kann und muss, wie es angesichts der beschränkten Tragweite möglich ist, die ein System geheimer Überwachung für einen Rechtsbehelf mit sich bringt. Aus den beiden zitierten Urteilen Big Brother Watch und andere und Centrum för rättvisa ergeben sich die folgenden Anforderungen: Der Rechtsbehelf muss vor einer Behörde erhoben werden können, die, wenn auch nicht notwendig richterlich, so doch von der Exekutive unabhängig ist. Zudem ist die Fairness des Verfahrens sicherzustellen und das Verfahren so weit als möglich kontradiktorisch auszugestalten. Die Entscheidungen eines solchen Organs sollen schliesslich begründet und rechtlich verbindlich sein (zit. Urteile Big Brother Watch und andere, §§ 357 ff. und Centrum för rättvisa, §§ 272 f. und 355; vgl. zudem zit. Urteil Klass, § 69 und BGE 138 I 6 E. 6, insbesondere 6.2).

E. 22.2.1

Gemäss dem Sachverhalt, der dem Urteil Big Brother Watch und andere zu Grunde lag, konnten Überwachungsmassnahmen von Betroffenen vor einem unabhängigen Spezialgericht, dem sogenannten Investigatory Powers Tribunal (nachfolgend: IPT), gerügt werden. Jede Person, die glaubte, einer Überwachung unterworfen zu sein, war berechtigt, einen Antrag an das IPT stellen. Dieses verfügte insoweit über eine weitreichende und damit hinreichende Zuständigkeit, die nicht von einer (nachträglichen) Benachrichtigung betroffener Personen abhing. Die Mitglieder des IPT mussten ein hohes Richteramt innehaben oder qualifizierte Rechtsanwälte sein. Die Behörden waren sodann verpflichtet, dem IPT alle benötigten Dokumente offenzulegen. Ferner konnte das IPT mündliche und wenn möglich öffentliche Verhandlungen durchführen; war eine öffentliche Verhandlung nicht möglich, konnte das Gericht einen sogenannten Councel to the tribunal bitten, im Namen des Klägers Stellung zu nehmen und auf diese Weise dessen Interessen zu vertreten. Schliesslich kam dem IPT die Befugnis zu, mit seinem Entscheid eine Ermächtigung zur Überwachung aufzuheben beziehungsweise zu widerrufen und es konnte die Vernichtung

von erfassten Daten anordnen. Der EGMR hielt in diesem Zusammenhang schliesslich fest (zit. Urteil Big Brother Watch und andere, § 413): [...] Enfin, la publication des décisions de l'IPT sur son propre site internet dédié accroissait le degré de contrôle exercé sur les activités de surveillance secrète au Royaume-Uni [...]. Der EGMR kam insgesamt zum Ergebnis, die Möglichkeit der Beschwerde an das IPT biete jedem, der den Verdacht hatte, dass seine Kommunikation überwacht werde, einen wirksamen Rechtsbehelf (zum Ganzen zit. Urteil Big Brother Watch und andere, §§ 413 und 415).

E. 22.2.2

Demgegenüber sah das schwedische Recht gemäss dem zitierten Urteil Centrum för rättvisa keinen hinreichend wirksamen Rechtsbehelf vor. Nach dem damals geltenden Recht konnten sich Betroffene an die Aufsichtsbehörde wenden; ein Nachweis, dass sie möglicherweise von einer Massenüberwachung betroffen sind, war nicht erforderlich. Die Aufsichtsbehörde untersuchte in der Folge, ob die Kommunikation der betroffenen Person überwacht wurde und ob die Überwachung gegebenenfalls rechtmässig erfolgte. Sie war zudem befugt, zu entscheiden, dass die Überwachung einzustellen ist und die erfassten Daten zu vernichten sind. Hingegen teilte die Aufsichtsbehörde dem Antragsteller lediglich mit, dass eine Untersuchung durchgeführt worden war, ohne das Ergebnis ihrer Untersuchung und ihren Entscheid bekannt zu machen. Der Umstand, dass der Aufsichtsbehörde nicht nur die behördliche Kontrolle der nachrichtendienstlichen Tätigkeit oblag, sondern sie darüber hinaus auch für die Beurteilung nachträglicher Rechtsbehelfe sachlich zuständig war, konnte nach der Beurteilung des EGMR dazu führen, dass die Behörde ihre eigene Tätigkeit als Aufsichtsbehörde zu beurteilen hatte. Der Gerichtshof erkannt in dieser doppelten Funktion die Gefahr von Interessenkonflikten. Die Gefahr könne zwar durch eine effektive übergeordnete Aufsicht über die Aufsichtsbehörde gemindert werden, der Nachweis einer effektiven Oberaufsicht sei durch die Regierung jedoch nicht erbracht worden. In grundsätzlicher Weise hielt der EGMR sodann das Folgende fest, das auch hier von Bedeutung ist (zit. Urteil Centrum för rättvisa, § 361 [Hervorhebungen nur hier): Par ailleurs, la Cour considère qu'un système de contrôle a posteriori dans lequel l'autorité saisie ne rend pas des décisions motivées communiquées aux intéressés, ou au moins des décisions contenant une motivation accessible à un avocat spécial titulaire d'une habilitation de sécurité, dépend trop largement de l'initiative et de la persévérance de fonctionnaires opérant à l'abri des regards. Elle observe que dans le système suédois, aucun détail n'est communiqué au demandeur quant à la teneur et à l'issue du contrôle effectué par l'Inspection, laquelle semble ainsi bénéficier d'une grande latitude. Une décision motivée présente l'avantage indéniable de mettre à la disposition du public des indications quant à l'interprétation des règles juridiques applicables, aux limites à respecter et à la manière dont l'intérêt public et les droits individuels doivent être mis en balance dans le contexte spécifique de l'interception en masse de communications. Comme la Cour l'a noté dans l'arrêt Kennedy (précité, § 167), la publication de telles conclusions juridiques accroît le degré de contrôle exercé en la matière. [...] Das zum damaligen Zeitpunkt anwendbare schwedische Recht bot daher insgesamt keine hinreichende Gewähr dafür, dass Missbräuche, falls sie auftreten, aufgedeckt und beseitigt werden konnten. Ins Gewicht fielen dabei die Doppelrolle der Aufsichtsbehörde sowie die fehlende Möglichkeit, auf Beschwerde hin einen begründeten Entscheid bezüglich der (vermuteten) Überwachung der eigenen Kommunikation zu erhalten. Der Gerichtshof wies schliesslich auf die Problematik hin, dass er in verschiedener Hinsicht nur in unzureichendem Mass über die tatsächliche Praxis der Massenüberwachung in Schweden informiert worden war (zit. Urteil Centrum

för rättvisa, §§ 354-364).

E. 22.3

Auch nach der Rechtsprechung des deutschen Bundesverfassungsgerichts kommt der unabhängigen Kontrolle und im speziellen der Kontrolle durch eine «gerichtsähnlich ausgestaltete Stelle» im Zusammenhang mit einer Massenüberwachung besondere Bedeutung zu (vgl. hierzu bereits vorstehend E. 19.2). Das Gericht unterscheidet dabei - anders als der EGMR - zwischen der verfassungsrechtlichen Rechtsschutzgarantie und der erwähnten gerichtsähnlichen Kontrolle. Diese Unterscheidung geht zurück auf das deutsche Grundgesetz. Dessen Art. 10 Abs. 2 Satz 2 hat folgenden Wortlaut (abrufbar unter < www.gesetze-im-internet.de > Gesetze/Verordnungen > GG): [...] Dient die Beschränkung [des Brief-, Post- und Fernmeldeverkehrs] dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt. Entsprechend hielt das deutsche Bundesverfassungsgericht im Rahmen seiner grundsätzlichen Ausführungen zur unabhängigen Kontrolle im Zusammenhang mit einer Massenüberwachung fest (zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung, Rz. 280 mit Hinweis auf das Urteil des EGMR Big Brother Watch und andere gegen Grossbritannien vom 13. September 2018, Nr. 58170/13, §§ 249 ff.): Bezogen auf die gerichtsähnliche Kontrolle wird der Gesetzgeber auch zu prüfen haben, ob Personen, die plausibel machen können, von Überwachungsmaßnahmen möglicherweise betroffen gewesen zu sein, das Recht eingeräumt werden kann, diesbezüglich mit eigenen Verfahrensrechten eine objektivrechtliche Kontrolle anzustoßen. Im Rahmen der hier in Frage stehenden objektivrechtlichen Kontrolle, die nicht als Verwirklichung der verfassungsrechtlichen Rechtsschutzgarantie zu verstehen ist und die förmliche Eröffnung des Rechtswegs [...] unberührt lässt, steht die Verfassung einer Ausgestaltung als Verfahren unter zumindest partiellem Ausschluss des Betroffenen und der Öffentlichkeit (in camera) nicht von vornherein entgegen. Dies gilt jedenfalls dann, wenn der Ausschluss erforderlich ist, um auf diesem Weg eine Kontrolle zu eröffnen, die andernfalls gar nicht möglich und verfassungsrechtlich deshalb auch nicht geboten wäre [...]. Das Bundesverfassungsgericht trägt damit dem Umstand Rechnung, dass die justizielle Kontrolle von Nachrichtendiensten einer sachbereichsspezifischen Limitierung unterworfen ist: Für eine wirksame Erfüllung ihrer Aufgaben seien Nachrichtendienste auf Geheimhaltung angewiesen. Eine Offenlegung von (konkreten) Informationen betreffend etwa die Aufklärungsmethoden und Erkenntnisquellen könne die Aufgabenerfüllung beeinträchtigen. Auf der anderen Seite setzten Rechtsschutz und gerichtliche Kontrolle grundsätzlich Publizität voraus. Geheimhaltung wirke insofern als faktisches Hindernis für den Zugang zum Gericht. Das deutsche Bundesverfassungsgericht kam in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung zu dem Ergebnis, dass die (damalige) gesetzliche Ausgestaltung der unabhängigen nachträglichen Kontrolle der strategischen Fernmeldeüberwachung den verfassungsrechtlichen Anforderungen nicht vollumfänglich gerecht wird. Es hielt zunächst fest, dass eine eng begrenzte Auskunftspflicht und auch das Fehlen von Benachrichtigungspflichten für sich betrachtet im betreffenden Kontext nicht zu beanstanden seien. Als Ausgleich für die Offenheit der Vorschriften und den faktisch erheblich eingeschränkten Rechtsschutz bedürfe es jedoch einer ausgebauten unabhängigen objektivrechtlichen Kontrolle. Eine solche könne mit Blick auf die Befugnisse und die

organisatorische sowie institutionelle Ausgestaltung nicht durch den Bundesbeauftragten für den Datenschutz in der verfassungsrechtlich gebotenen Weise sichergestellt werden (zit. Urteil des deutschen Bundesverfassungsgerichts zur Ausland-Ausland-Aufklärung, Rz. 324). Im Zuge der Beurteilung der Inland-Ausland-Aufklärung kritisierte das Bundesverfassungsgericht, dass die für die nachträgliche Kontrolle zuständige G 10-Kommission nebenamtlich und nicht wie verfassungsrechtlich geboten hauptamtlich tätigt ist; als Ersatz für den in erheblichem Mass eingeschränkten subjektiven Rechtsschutz sei eine «fachlich kompetente, professionalisierte gerichtsähnliche Kontrolle» erforderlich, die «materiell und verfahrensmässig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll ist». Hierfür reiche es nicht aus, die Durchführung der Kontrolle im Wesentlichen auf eine ehrenamtliche Amtsausübung zu stützen. Zudem sei nicht gesetzlich sichergestellt, dass dem Kontrollorgan auch Mitglieder mit richterlicher Erfahrung angehören. Das Bundesverfassungsgericht weist schliesslich darauf hin, dass der deutsche Bundesnachrichtendienst gesetzlich nicht verpflichtet sei, Überwachungsmassnahmen, sogenannte Beschränkungsanordnungen, in jedem Fall umfassend zu begründen. Eine umfassende nachträgliche Kontrolle wurde daher auch insoweit nicht in hinreichendem Mass ermöglicht (vgl. zit. Beschluss des deutschen Bundesverfassungsgerichts zur Inland-Ausland-Aufklärung, Rz. 207-210). Vor diesem Hintergrund enthalten die nunmehr für die strategische Fernmeldeaufklärung anwendbaren gesetzlichen Bestimmungen eine differenzierte Regelung. Einerseits ist anstelle des Anspruchs auf Auskunft über die Bearbeitung eigener Personendaten ein sogenanntes Ersatzrecht vorgesehen. Demnach ist eine Person im Falle der Verweigerung einer inhaltlichen Auskunft berechtigt, sich an den Bundesbeauftragten für den Datenschutz zu wenden, damit dieser beziehungsweise diese prüfe, ob eine Datenbearbeitung rechtmässig erfolge (vgl. § 9 des Gesetzes über den Bundesnachrichtendienst [BND-Gesetz; BNDG] unter Verweis auf § 15 des Bundesverfassungsschutzgesetzes [BVerfSchG], abrufbar unter < www.gesetze-im-internet.de > Gesetze/Verordnungen > BNDG). Andererseits steht gegen die Ablehnung einer Auskunftserteilung entsprechend der verfassungsrechtlichen Rechtsschutzgarantie die förmliche Eröffnung des Rechtsweges offen, wobei im Falle von Geheimhaltungsinteressen über die Offenlegung von Unterlagen beziehungsweise das Erteilung einer Auskunft auch hier unter Ausschluss des Betroffenen und der Öffentlichkeit und damit sogenannt in camera entschieden wird (vgl. Otto Mallmann, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 15 BVerfSchG Rz. 28-31; vgl. auch Bertold Huber, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 15 Artikel 10-Gesetz Rz. 35 ff.).

E. 23.1

Nach schweizerischem Recht stehen zu Beginn der unabhängigen nachträglichen Überprüfung das datenschutzrechtliche Auskunftsrecht gemäss Art. 25 Abs. 1 DSG beziehungsweise die datenschutzrechtlichen Ansprüche gemäss Art. 41 DSG. Die Auskunftserteilung kann jedoch aufgeschoben werden. Für diesen Fall sieht auch das schweizerische Recht einen Rechtsbehelf beziehungsweise einen Kontrollmechanismus vor, das sogenannte indirekte Auskunftsrecht (vgl. zum Begriff BGE 138 I 6 E. 3.3.2 für das vormals anwendbare, dem Grundsatz nach aber mit dem geltenden Recht übereinstimmende BWIS). Darauf ist im Folgenden einzugehen.

E. 23.2.1

Das hier anwendbare Nachrichtendienstgesetz enthält im 4. Abschnitt des 4. Kapitels besondere Bestimmungen über den Datenschutz. Diese gehen als lex specialis dem im Übrigen anwendbaren Datenschutzrecht vor. Verlangt eine Person Auskunft darüber, ob die Vorinstanz Daten über sie bearbeitet, ist danach zu unterschieden, in welchem der nachrichtendienstlichen Informationssysteme Daten bearbeitet werden. Das Auskunftsrecht für die in Art. 63 Abs. 1 NDG genannten Informationssysteme richtet sich nach den Bestimmungen des Datenschutzgesetzes, während Art. 63 Abs. 2 NDG als lex specialis zu den Bestimmungen des Datenschutzgesetzes für die weiteren Informationssysteme die Möglichkeit eines Aufschubs der Auskunft und damit auch des Rechtsschutzes vorsieht. Die Vorinstanz bearbeitet Resultate aus der Kabelaufklärung praxisgemäss im integralen Analysesystem (IASA NDB). Für dieses Informationssystem und auch für die weiteren hier betroffenen Informationssysteme sieht die Bestimmung von Art. 63 Abs. 2 NDG die Möglichkeit eines Aufschubs der Auskunft vor. Demnach wird die Auskunft aufgeschoben, wenn und soweit überwiegende, in den Akten zu begründende Interessen an einer Geheimhaltung bestehen im Zusammenhang mit der Erfüllung einer Aufgabe nach Art. 6 NDG, einer Strafverfolgung oder einem anderen Untersuchungsverfahren (Art. 63 Abs. 2 Bst. a NDG). Ebenfalls aufzuschieben ist die Auskunft, wenn und soweit dies wegen überwiegender Interessen Dritter erforderlich ist (Art. 63 Abs. 2 Bst. b NDG) oder wenn über die gesuchstellende Person keine Daten bearbeitet werden (Art. 63 Abs. 2 Bst. c NDG). Die Vorinstanz teilt der gesuchstellenden Person den Aufschub der Auskunft mit und weist sie darauf hin, dass sie das Recht hat, vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB zu verlangen, dass er prüfe, ob allfällige Daten rechtmässig bearbeitet werden und ob überwiegende Geheimhaltungsinteressen den Aufschub rechtfertigen (Art. 63 Abs. 3 NDG). Der Beauftragte führt auf Verlangen die Prüfung durch und teilt der gesuchstellenden Person mit, dass entweder in Bezug auf sie keine Daten unrechtmässig bearbeitet werden, oder dass er bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft Fehler festgestellt und eine Untersuchung nach Art. 49 DSG eröffnet hat (Art. 64 Abs. 2 NDG). Stellt der Beauftragte im Rahmen seiner Untersuchung Fehler bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft fest, so verfügt er, dass die Vorinstanz diese behebt (Art. 64 Abs. 4 NDG; vgl. auch Art. 51 DSG). Legt die gesuchstellende Person glaubhaft dar, dass ihr bei einem Aufschub der Auskunft ein erheblicher, nicht wiedergutzumachender Schaden erwächst, so kann der Beauftragte gemäss Art. 64 Abs. 4 NDG verfügen, dass die Vorinstanz ausnahmsweise sofort Auskunft erteilt, sofern damit keine Gefährdung der inneren oder äusseren Sicherheit verbunden ist. Gemäss Art. 66 Abs. 1 NDG sind schliesslich die Mitteilungen nach den Art. 63 Abs. 3 NDG und Art. 64 Abs. 2 NDG stets gleichlautend und werden nicht begründet. Sie können nicht mit einem Rechtsmittel angefochten werden (Art. 66 Abs. 2 NDG). Im Folgenden ist näher auf das Mittel der förmlichen Untersuchung einzugehen. Gemäss Art. 49 Abs. 1 DSG eröffnet der Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB von Amtes wegen oder auf Anzeige eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Im Zusammenhang hat der Untersuchung hat der Beauftragte insbesondere Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeit und Personendaten, die für die Untersuchung erforderlich sind (Art. 50 Abs. 1 Bst. a DSG). Liegt eine Verletzung von Datenschutzvorschriften vor, kann der Beauftragte insbesondere verfügen, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird und die Personendaten ganz oder teilweise gelöscht

oder vernichtet werden (Art. 51 Abs. 1 DSG). Das Untersuchungsverfahren sowie Verfügungen nach den Art. 50 und Art. 51 DSG richten sich nach dem VwVG (Art. 52 Abs. 1 DSG). Verfahrenspartei ist nur das Bundesorgan, gegen das eine Untersuchung eröffnet wurde (Art. 52 Abs. 2 DSG). Gegen Verfügungen des Beauftragten steht die Beschwerde an das Bundesverwaltungsgericht offen (Art. 31 VGG). Gemäss Art. 52 Abs. 3 DSG ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB berechtigt, Beschwerdeentscheide des Bundesverwaltungsgerichts anzufechten.

E. 23.2.2

Der Entscheid darüber, ob die Auskunft betreffend die in Art. 63 Abs. 2 NDG genannten nachrichtendienstlichen Informationssysteme aufzuschieben ist, steht nach Wortlaut des Gesetzes unter dem Vorbehalt einer Interessenabwägung; die Auskunft ist aufzuschieben, wenn und soweit überwiegende Interessen an einer Geheimhaltung bestehen. Nach der Rechtsprechung ist die Interessenabwägung - auch und gerade im Falle eines Aufschubs der Auskunft - zu Händen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB transparent zu machen, ansonsten die indirekte Auskunft beziehungsweise die Möglichkeit der indirekten Überprüfung ohne Gehalt bliebe. Die Pflicht zur Begründung dient auch hier der Selbstkontrolle: Der Anspruch auf Auskunft ergibt sich aus Art. 13 BV und Art. 8 EMRK. Er ist unentbehrliche Voraussetzung für die Verwirklichung des Schutzes des Privatlebens und eine Verweigerung beziehungsweise ein Aufschub der Auskunft ist auf das zeitlich und sachlich unbedingt Notwendige zu beschränken (Urteil des BVGer A-4729/2020 vom 24. November 2022 E. 5.3.2 und 5.4.3 mit Hinweisen). Besteht bereits im Zeitpunkt des Gesuchs kein legitimes Geheimhaltungsinteresse im Sinne von Art. 63 Abs. 2 NDG (mehr), darf die Auskunft somit nicht aufgeschoben werden. Vielmehr ist das Auskunftsrecht unter diesen Umständen nach den Bestimmungen des Datenschutzgesetzes zu beurteilen (vgl. Urteil des BVGer A-4725/2020 vom 1. Februar 2023 E. 7.3.4 f.). Gemäss Art. 63 Abs. 4 NDG erteilt die Vorinstanz der gesuchstellenden Person nach dem Datenschutzgesetz Auskunft, sobald kein Geheimhaltungsinteresse mehr an Daten besteht, spätestens aber nach Ablauf der Aufbewahrungsdauer, und sofern die Erteilung der Auskunft nicht mit übermässigem Aufwand verbunden ist. Die nachträgliche Auskunftserteilung ermöglicht es, die Offenlegung sensibler Informationen zu vermeiden, so lange überwiegende Geheimhaltungsinteressen bestehen, ohne effektiven Rechtsschutz vollständig auszuschliessen; ist die Dauer einer zulässigen Aufbewahrung abgelaufen oder sind die überwiegenden Geheimhaltungsinteressen entfallen, findet das Datenschutzgesetz Anwendung und es eröffnet sich der ordentliche Rechtsmittelweg. Nach der Rechtsprechung hat die Vorinstanz die gesuchstellende Person bei Dahinfallen der Geheimhaltungsinteressen von Amtes wegen zu informieren und ein zuvor gestelltes Auskunftsgesuch nunmehr nach den Bestimmungen des Datenschutzgesetzes zu behandeln, ohne dass hierfür ein erneuter Antrag erforderliche wäre (vgl. BGE 138 I 6 E. 3.3.5 und 7.5, insbes. E. 7.5.1; Urteil des BVGer A-4725/2020 vom 1. Februar 2023 E. 7.3.4 f.).

E. 23.3.1

Der Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB äussert sich im Rahmen seiner Antworten zu den Fragenkatalogen zu seiner Praxis im Zusammenhang mit dem indirekten Auskunftsrecht. Die erste Stellungnahme des Beauftragten erfolgte vor Inkrafttreten des totalrevidierten Datenschutzgesetzes und der gleichzeitig mit der Totalrevision des Datenschutzgesetzes beschlossenen weiteren Gesetzesänderungen; zusammen mit der Totalrevision des Datenschutzgesetzes wurde auch das

Nachrichtendienstgesetz geändert. Die Änderungen betrafen insbesondere das indirekte Auskunftsrecht. Unter dem vormals geltenden Recht bestand für die gesuchstellender Person zusätzlich zur indirekten Auskunft durch den Beauftragten die Möglichkeit, vom Bundesverwaltungsgericht zu verlangen, dass dieses die Mittelung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB und den Vollzug der Empfehlung überprüfe. Auch die Mitteilung des Bundesveraltungsgerichts war stets gleichlautend und konnte nicht mit einem Rechtsmittel angefochten werden (vgl. aArt. 64 Abs. 3, aArt. 65 und aArt. 66 NDG [AS 2017 4124 f.]). Zudem eröffnete der Beauftragte gemäss dem vormals geltenden Recht keine Untersuchung gemäss Art. 49 DSG. Vielmehr sprach er, wenn er bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft Fehler festgestellt hatte, eine Empfehlung im Sinne von Art. 27 aDSG zu deren Behebung an die Vorinstanz aus (aArt. 64 Abs. 2 und 4 NDG [AS 2017 4124]). In seinem Kern ist daher die indirekte Auskunft des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten auch mit der Totalrevision des Datenschutzgesetzes dieselbe geblieben, weshalb grundsätzlich auch die Stellungnahme des Beauftragten vom 11. November 2022 weiterhin von Bedeutung ist.

E. 23.3.2

Gemäss den Ausführungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB kommt ihm beziehungsweise seiner Prüfungskompetenz gemäss Art. 64 NDG eine entscheidende Rolle zur Wahrnehmung der Rechte der gesuchstellenden Person unter gleichzeitiger Wahrung von berechtigten nachrichtendienstlichen Geheimhaltungsinteressen zu. Bearbeite die Vorinstanz keine Daten über die gesuchstellende Person, erstelle die Vorinstanz zuhanden des Beauftragten eine Bescheinigung über die Nichtverzeichnung. In solchen Fällen prüfe der Beauftragte, ob der gesuchstellenden Person bei einem Aufschub der Auskunft ein schwerwiegender und nicht wiedergutzumachender Nachteil im Sinne von Art. 64 Abs. 5 NDG droht und dieser Nachteil glaubhaft dargelegt ist. Gegebenenfalls teile er der Vorinstanz die Absicht mit, eine Empfehlung auszusprechen (sog. informelle Empfehlung), wonach der gesuchstellenden Person unverzüglich mitzuteilen sei, dass keine Daten über sie bearbeitet werden. Dies gebe der Vorinstanz ihrerseits die Möglichkeit, gegenüber dem Beauftragten darzulegen, weshalb eine sofortige Mitteilung über die Nichtverzeichnung aus Gründen der inneren oder äusseren Sicherheit zu unterbleiben habe. Informelle Empfehlungen seien stets befolgt worden, so dass bisher keine formelle Empfehlung habe ausgesprochen werden müssen. Für den Fall, dass Daten über die gesuchstellende Person bearbeitet werden, würden zwei Mitarbeitende des Beauftragten die betreffenden Personendaten vor Ort einsehen; die Personendaten würden den Mitarbeitenden des Beauftragten präsentiert, da dieser keinen eigenen Zugang zu den Informationssystemen der Vorinstanz habe. Auf Verlangen des Beauftragten hin suche die Vorinstanz im Beisein von dessen Mitarbeitenden in den Informationssystemen nach (weiteren) Informationen über die gesuchstellende Person. Anschliessend beurteile der Beauftragte die Rechtmässigkeit der Datenbearbeitung. Konkret werde geprüft, ob ein hinreichender Aufgabenbezug vorliegt und ob die Datenbearbeitungsschranken und die Aufbewahrungsfristen eingehalten werden. Die Einhaltung weiterer (interner) Vorgaben wie die Pflicht zur Protokollierung der Datenbearbeitung oder die Kennzeichnungspflicht von Daten mit einem Bezug zur Schweiz sei hingegen nicht Gegenstand der Überprüfung. Für den Fall, dass eine unrechtmässige Datenbearbeitung festgestellt werde, richte der Beauftragte zunächst wiederum eine informelle Empfehlung an die Vorinstanz, wobei auch in dieser Hinsicht bisher keine formelle Empfehlung habe ausgesprochen werden müssen. Abschliessend weist der

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB darauf hin, dass die indirekte Auskunft unbefriedigend sei, weil die gesuchstellende Person daraus nicht einmal ableiten könne, ob überhaupt Daten über sie bearbeitet würden. Zudem könne er in der Rolle als Vertreter der gesuchstellenden Person mangels Kontextinformationen nicht (abschliessend) beurteilen, ob bestimmte Informationen richtig seien, womit das Recht auf Berichtigung unrichtiger Daten zumindest teilwiese seines Gehalts entleert werde (zum Ganzen Stellungnahmen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB vom 27. Oktober 2023 und vom 11. November 2022).

E. 24.1

Die Beurteilung des Verfahrens für eine unabhängige nachträgliche Überprüfung der Einhaltung der Garantien einschliesslich der Befugnisse der zuständigen Behörde für den Fall der Nichteinhaltung ist gemäss der Rechtsprechung der Grossen Kammer des EGMR auf die folgenden Kriterien abzustützen: - Unabhängigkeit der Behörde - Zuständigkeit der Behörde - Ausgestaltung des Verfahrens - Befugnisse der Behörde

E. 24.2.1

Eine Benachrichtigung von Personen, deren Kommunikation im Rahmen einer Funk- und Kabelaufklärung überwacht wurde, ist nicht vorgeschrieben; die Funk- und Kabelaufklärung sind Instrumente der anlasslosen Massenüberwachung, weshalb eine Pflicht zur (nachträglichen) Benachrichtigung nicht mit vernünftigem Aufwand umsetzbar wäre. Auch der EGMR macht in seiner Rechtsprechung die Wirksamkeit einer unabhängigen nachträglichen Überprüfung nicht davon abhängig, ob eine Benachrichtigung des Betroffenen über die Datenbearbeitung erfolgt (vgl. vorstehend E. 22.1 f.). Damit fehlt hier jedoch ein an sich wirksames Mittel gegen Missbrauch, das es Betroffenen ermöglichen würde, den Rechtsweg zu beschreiten (vgl. auch BGE 140 I 381 E. 4.5.1). Zu prüfen ist, ob eine nachträgliche Überprüfung einer Überwachung beziehungsweise Datenbearbeitung auch auf anderem Weg erreicht werden kann. Nach dem anwendbaren Recht hat jede Person die Möglichkeit, Auskunft darüber zu verlangen, ob Personendaten über sie bearbeitet werden (Art. 25 Abs. 1 DSG); an die Auskunft knüpfen die datenschutzrechtlichen Ansprüche gemäss Art. 41 DSG an. Das anwendbare Recht schliesst im Zusammenhang mit der Bearbeitung von Personendaten aus Resultaten der Funk- und Kabelaufklärung somit ordentlichen Rechtsschutz (im Rahmen des Auskunftsrechts) nicht aus. Zwar kann die Erteilung der Auskunft aufgrund überwiegender entgegenstehender Interessen aufgeschoben werden, bei Fehlen von oder Wegfall der Geheimhaltungsinteressen ist jedoch nach den Bestimmungen des Datenschutzgesetzes Auskunft zu erteilen, wodurch sich der ordentliche Rechtsmittelweg öffnet (vgl. vorstehend E. 23.2.2). Ein Aufschub der Auskunft ist vor dem Hintergrund, dass der Informationsbeschaffung durch die Vorinstanz (im Rahmen der Funk- und Kabelaufklärung) ihrer Natur nach Geheimnischarakter zukommt, grundsätzlich mit Art. 8 EMRK vereinbar, sofern insgesamt in hinreichendem Mass Schutz vor Missbrauch besteht (vgl. BGE 138 I 6 insbes. E. 5 und E. 7.5). Hier ist jedoch im Sinne der Rechtsprechung des EGMR zur Massenüberwachung zu beachten, dass Daten im integralen Analysesystem (IASA NDB) - sofern sie zur Aufgabenerfüllung benötigt werden - über sehr lange Zeit aufbewahrt werden dürfen. Die Aufbewahrungsfrist beträgt für Quellendokumente je nach Themenbereich bis zu 45 Jahre und für Originaldokumente bis zu 15 Jahre. Die Dauer der Bearbeitung von Resultaten aus der Kabelaufklärung kommt damit einer unbefristeten Aufbewahrung im Sinne der Rechtsprechung des EGMR zumindest sehr nahe (vgl.

vorstehend E. 18.2.1 und E. 18.3.2). Es ist sodann davon auszugehen, dass während der Dauer der Aufbewahrung grundsätzlich Geheimhaltungsinteressen bestehen und daher die Auskunft für die Dauer der Aufbewahrung der Daten aufzuschieben ist. Unter diesen Umständen kann nicht ohne Weiteres gesagt werden, es bestehe im Falle eines Aufschubs effektiver Rechtsschutz im Rahmen der späteren Erteilung der Auskunft nach den Bestimmungen des Datenschutzgesetzes. Dies muss umso mehr gelten, als sich das Auskunftsrecht direkt aus Art. 13 in Verbindung mit Art. 8 EMRK ergibt und der Aufschub bereits eine erhebliche Einschränkung darstellt (vgl. zum Ganzen Urteil des BGer 1C_493/2023 vom 26. November 2024 E. 4.4 und E. 5). Das Nachrichtendienstgesetz sieht vor diesem Hintergrund mit dem indirekten Auskunftsrecht einen Kontrollmechanismus vor, vergleichbar dem im deutschen Recht festgeschriebenen Ersatzrecht, der Beschwerde an die G 10-Kommission. Im Folgenden ist unter Berücksichtigung insbesondere auch des Verhältnismässigkeitsgrundsatzes zu prüfen, ob durch die indirekte Auskunft in hinreichendem Mass eine nachträgliche Überprüfung im Sinne der Rechtsprechung des EGMR zur Massenüberwachung (zit. Urteile Big Brother Watch und andere und Centrum för rättivsa) ermöglicht wird.

E. 24.2.2

Die unabhängige nachträgliche Überprüfung der vermuteten Bearbeitung von Personendaten der Beschwerdeführenden erfolgt nach der Konzeption des Nachrichtendienstgesetzes auf dem Weg der indirekten Auskunft durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB. Die oder der Beauftragte übt ihre oder seine Funktion gemäss Art. 43 Abs. 4 DSG unabhängig aus, ohne Weisungen einer Behörde oder eines Dritten einzuholen oder entgegenzunehmen. Die gesuchstellende Person kann vom Beauftragten verlangen, dass er prüfe, ob allfällige Daten rechtmässig bearbeitet werden, und ob überwiegende Geheimhaltungsinteressen den Aufschub der Auskunft rechtfertigen (Art. 63 Abs. 3 NDG). Diese Möglichkeit steht jeder Person zu, ohne dass sie nachweisen muss, möglicherweise von einer Überwachung betroffen (gewesen) zu sein. Der Beauftragte führt die Prüfung sodann inhaltlich durch, teilt der gesuchstellenden Person jedoch stets gleichlautend mit, dass entweder in Bezug auf sie keine Daten unrechtmässig bearbeitet werden oder dass er bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft Fehler festgestellt und - nach neuem, geltenden Datenschutzrecht - eine Untersuchung nach Art. 49 DSG eröffnet hat (vgl. zur Frage, welches Datenschutzrecht anwendbar und dem vorliegenden Entscheid zu Grunde zu legen ist, vorstehend E. 4.2). Stellt der Beauftragte bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft Fehler fest, so verfügt er, dass die Vorinstanz diese behebt (Art. 64 Abs. 4 NDG). Die nachträgliche Überprüfung im Rahmen des indirekten Auskunftsrechts erfolgt somit durch eine unabhängige Behörde (vgl. hierzu das Urteil des BVGer A-4781/2019 vom 17. Juni 2020 E. 3.5.3.1), die Zugang zu allen zweckdienlichen Informationen und Unterlagen hat und die nach neuem Datenschutzrecht, wenn sie bei der Datenbearbeitung oder betreffend den Aufschub der Auskunft Fehler feststellt, verfügungsbefugt ist. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB ist zudem umfassend zuständig und es besteht ein Anspruch auf Prüfung der Vorbringen; es ist jedermann berechtigt, ein Gesuch um Auskunft zu stellen und vom Beauftragten eine Überprüfung der Rechtmässigkeit einer allfälligen Datenbearbeitung zu verlangen. Gleichwohl vermag die Ausgestaltung des Verfahrens den Anforderungen gemäss der Rechtsprechung des EGMR in verschiedener Hinsicht nicht zu genügen. Von grundsätzlicher Bedeutung ist zunächst, dass das Verfahren nicht kontradiktorisch

ausgestaltet ist; die indirekte Auskunft wird nicht im Rahmen eines Verwaltungsverfahrens unter Gewährung von Parteirechten erteilt und auch in einer allfälligen Untersuchung durch den Beauftragten ist Partei nur das Bundesorgan, gegen das eine Untersuchung eröffnet worden ist (Art. 52 Abs. 2 DSG), während der gesuchstellenden Person auch hier - wie schon nach altem Datenschutzrecht - keine Parteirechte zukommen. Gleichwohl, das heisst trotz des fehlenden kontradiktorischen Charakters des Verfahrens der indirekten Auskunft beziehungsweise des daran allenfalls anschliessenden Untersuchungsverfahrens, sieht das anwendbare Recht - anders als etwa im Vereinigten Königreich nach damaligem Recht (vgl. hierzu vorstehend E. 22.2.1) - keine Prozessvertretung oder andere solide Verfahrensgarantien vor. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB erlässt sodann nicht in jedem Fall einen begründeten Entscheid beziehungsweise eine Verfügung (Art. 64 Abs. 4 NDG) und die Entscheide werden abgesehen von Fällen, die von allgemeinem Interesse sind (Art. 57 Abs. 2 DSG), nicht veröffentlicht. Insgesamt kann die gesuchstellende Person somit zwar durch Gesuch eine Überprüfung veranlassen, sie erhält hierbei jedoch weder Parteirechte noch inhaltlich Auskunft (im Rahmen eines begründeten Entscheids). Damit bietet das indirekte Auskunftsrecht keine ausreichende Grundlage für ein Vertrauen der Öffentlichkeit darin, dass Missbräuche, falls sie auftreten, aufgedeckt und beseitigt werden. Es gewährleistet für sich allein nicht in hinreichendem Mass eine nachträgliche Überprüfung im Sinne der Rechtsprechung des EGMR zur Massenüberwachung der Telekommunikation (vgl. in diesem Sinne auch das zit. Urteil Centrum för rättvisa, § 361; vgl. zudem BGE 149 I 218 E. 6.3.2). An diesem Ergebnis ändert auch nichts, dass gemäss dem Urteil des Bundesgerichts 1C_289/2009 vom 2. November 2011 (teilweise publiziert in BGE 138 I 6) das indirekte Auskunftsrecht einen hinreichenden Rechtsbehelf im Sinne von Art. 13 EMRK bietet. Zu beurteilen war in jenem Verfahren, ob der Aufschub einer Auskunft im konkreten Fall aus Gründen der inneren und äusseren Sicherheit zulässig war. Das Bundesgericht bejahte dies unter der Voraussetzung, dass als Ausgleich ein hinreichender Rechtsbehelf zum Schutz vor Missbrauch zur Verfügung stehe und erkannte einen solchen im indirekten Auskunftsrecht. Zudem ging es davon aus, dass nach Wegfall der Geheimhaltungsinteressen von Amtes wegen Auskunft erteilt und damit nachträglicher Rechtsschutz möglich ist. Das Urteil 1C_289/2009 erging somit in einem anderen Kontext und zeitlich vor den hier massgebenden Urteilen der Grossen Kammer des EGMR, weshalb daraus nicht ohne Weiteres abgeleitet werden kann, mit dem indirekten Auskunftsrecht werde in hinreichendem Mass eine nachträgliche Überprüfung von Informationsbeschaffungen ermöglicht. Vielmehr ist das in der Schweiz hinsichtlich der nachträglichen Überprüfung geltende Regime des indirekten Auskunftsrechts mit dem schwedischen Recht vergleichbar, das dem zitierten Urteil Centrum för rättvisa zu Grunde lag. Der EGMR hielt hierzu fest, die Wirksamkeit einer auf diese Weise, das heisst ohne Parteirechte und ohne Öffentlichkeit ausgestalteten nachträglichen Überprüfung «dépend trop largement de l'initiative et de la persévérance de fonctionnaires opérant à l'abri des regards» (zit. Urteil Centrum för rättvisa, § 361).

E. 24.2.3

In Betracht zu ziehen ist zudem, dass auch das Datenschutzrecht den Aufschub oder die Verweigerung einer Auskunft aufgrund überwiegender Geheimhaltungsinteressen zulässt (vgl. Art. 26 Abs. 2 Bst. b DSG). Im Unterscheid zum Aufschub der Auskunft gestützt auf das Nachrichtendienstgesetz ergeht der Entscheid nach dem Datenschutzgesetz in Form einer Verfügung nach dem VwVG. Gegen diese steht der ordentliche Rechtsmittelweg offen. Der Rechtsmittelinstanz obliegt es alsdann, zu prüfen, ob der Auskunftserteilung

überwiegende öffentliche Interessen (der inneren und äusseren Sicherheit) entgegenstehen. In diesem Prüfverfahren wird keine Akteneinsicht gewährt (Urteil des BGer 1C_597/2020 vom 14. Juni 2021 E. 5 [nicht publiziert in BGE 147 II 408]). Die Rechtsmittelinstanz beurteilt anhand der ihr vorliegenden Akten, ob das Auskunftsrecht zu Recht eingeschränkt wurde. In ihrer Urteilsbegründung hat sie den berechtigen Geheimhaltungsinteressen Rechnung zu tragen und daher unter Umständen auf eine umschreibende Begründung der Geheimhaltungsgründe auszuweichen (vgl. Urteil des BGer 1C_257/2022 vom 7. Juni 2023 E. 6.3). Der Rechtsmittelinstanz kommt mithin in einem derartigen Verfahren auch die Aufgabe zu, die Interessen der Partei, die selbst keine Einsicht in die Akten hat, zu wahren. Für die betroffene Person bietet ein solches Verfahren nach dem Datenschutzgesetz den Vorteil, dass sie die Umstände der Einschränkung des Auskunftsrechts durch eine gerichtliche Instanz in einem kontradiktorischen Rechtsmittelverfahren überprüfen lassen kann. Im Rechtsmittelverfahren ergeht sodann - unter Berücksichtigung der Geheimhaltungsinteressen - ein begründetes Urteil und für den Fall, dass ein Gesuch um Auskunft (durch die Rechtsmittelinstanz) gutgeheissen würde, stünden der gesuchstellenden Person hiernach die datenschutzrechtlichen Ansprüche gemäss Art. 41 DSG offen. Zu einem solchen Ergebnis führt das indirekte Auskunftsrecht nicht; selbst wenn der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB eine unrechtmässige Datenbearbeitung feststellen würde, erhielte die gesuchstellende Person hierzu keine Angaben und der Zugang zu den datenschutzrechtlichen Ansprüchen gemäss Art. 41 DSG bliebe während des Aufschubs der Auskunft gestützt auf das Nachrichtendienstgesetz verwehrt (vgl. hierzu vorstehend E. 23.2.1). Vor diesem Hintergrund erscheint daher das indirekte Auskunftsrecht auch nicht hinreichend wirksam (vgl. zum Ganzen BGE 149 I 218 E. 6.3.2; BGE 147 II 408 E. 6, insbes. E. 6.3; Urteil des BGer 1C_493/2023 vom 26. November 2024 E. 5, insbes. E. 5.6; zudem Urteil des BGer 1C_522/2018 vom 8. März 2019 E. 3.3; ferner die Urteile des BVGer B-2399/2021 vom 11. April 2025 E. 4.3.2 und E. 7.2.2.2 sowie A-4725/2020 vom 1. Februar 2023 E. 7.4.3; Waldmann/Oeschger, in: Praxiskommentar zum VwVG, 3. Aufl. 2023, Art. 28 Rz. 10). Insgesamt bestehen somit Anhaltspunkte, dass den berührten Interessen und insbesondere den Geheimhaltungsinteressen der Vorinstanz - vergleichbar der dem deutschen Recht zu Grunde liegenden Konzeption - auch beziehungsweise gerade im Rahmen eines datenschutzrechtlichen Verfahrens zur Beurteilung eines Auskunftsgesuchs hinreichend Rechnung getragen werden könnte (vgl. zum Erfordernis des hinreichenden Rechtsschutzes auch BGE 149 I 2 E. 2.1 und 3, insbes. E. 3.1).

E. 24.2.4

Mit der laufenden Revision des Nachrichtendienstgesetzes soll die Regelung des Auskunftsrechts vereinfacht werden. Neu könnte die Auskunft nur noch «ausnahmsweise und einzelfallbedingt» aufgeschoben werden. Der Aufschub der Auskunft soll zudem künftig nach dem Datenschutzgesetz beurteilt werden; gemäss dem Vernehmlassungsentwurf kann die Vorinstanz «die Auskunft aus den Gründen nach Artikel 26 DSG verweigern, einschränken oder aufschieben». Ein ordentliches Verwaltungsverfahren unter Gewährung von Parteirechten würde jedoch auch weiterhin nicht durchgeführt. Vielmehr soll das indirekte Auskunftsrecht beibehalten werden, wobei die Möglichkeit, die Mitteilung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB vom Bundesverwaltungsgericht überprüfen zu lassen, wieder eingeführt würde; diese Möglichkeit war zuvor mit der Totalrevision des Datenschutzgesetzes gestrichen worden (Erläuternder Bericht Revision NDG S. 28 f.;

Vernehmlassungsvorlage zur Revision des Bundesgesetzes vom 25. September 2015 über den Nachrichtendienst, < www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2022 > VBS, abgerufen am 16. Oktober 2025). Anders als nach geltendem Recht (Art. 63 Abs. 2 Bst. c NDG) soll die Nichtverzeichnung einer auskunftsgesuchstellenden Person sofort mitgeteilt werden können.

E. 24.3

Zusammenfassend ergibt sich zum achten Prüfpunkt, dass das indirekte Auskunftsrecht durch den unabhängig handelnden Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB einen Mechanismus zum Schutz vor Missbrauch darstellt. Das Auskunftsrecht vermag im Sinne der Rechtsprechung des EGMR zur Massenüberwachung für sich alleine allerdings keine unabhängige nachträgliche Überprüfung zu gewährleisten. So erhält die gesuchstellende Person weder Parteirechte noch inhaltlich Auskunft; ein kontradiktorisches Verfahren oder zumindest eine Prozessvertretung für die gesuchstellende Person ist nicht vorgesehen. Die nachträgliche Überprüfung kann somit zwar durch die betroffene Person angestossen werden, die Überprüfung selbst erfolgt jedoch im Geheimen. Die Effektivität der Kontrolle hängt damit im Ergebnis (im Wesentlichen) und in den Worten des EGMR von der Beharrlichkeit der Mitarbeitenden des Beauftragten ab. Im Vergleich zu dem System, wie es der EGMR in seinem Urteil Big Brother Watch und andere zu beurteilen hatte, bietet das anwendbare Recht hier somit keinen hinreichenden Schutz vor Missbrauch und weist insoweit einen Mangel auf. Es bestehen sodann Anhaltspunkte, dass den berührten und insbesondere den Geheimhaltungsinteressen der Vorinstanz auch im Rahmen eines datenschutzrechtlichen Verfahrens zur Beurteilung eines Auskunftsgesuchs hinreichend Rechnung getragen werden könnte. In diesem Sinne ist im Rahmen der laufenden Revision denn auch eine Annäherung an das datenschutzrechtliche Auskunftsrecht vorgesehen und für den Fall, dass die gesuchstellende Person nicht verzeichnet ist, würde ihr zudem sofort Auskunft erteilt. Gesamtbeurteilung

E. 25.1

Die vermutete Bearbeitung von Personendaten der Beschwerdeführenden im Rahmen der Funk- und Kabelaufklärung beeinträchtigt diese in ihrem Privatleben (Art. 8 Ziff. 1 EMRK; Art. 13 Abs. 1 BV) und jedenfalls die Beschwerdeführenden 4 und 6 in ihrer Medienfreiheit (Art. 10 Ziff. 1 EMRK; Art. 17 BV; vgl. hierzu vorstehend E. 6). Die Beeinträchtigung kann gerechtfertigt werden (Art. 8 Ziff. 2 und Art. 10 Ziff. 2 EMRK; Art. 36 BV). Nach der Rechtsprechung der Grossen Kammer des EGMR setzt die Rechtfertigung einer Grundrechtsbeeinträchtigung durch ein Regime zur Massenüberwachung voraus, dass insgesamt ausreichende Garantien zum Schutz vor Missbrauch eines Regimes zur Massenüberwachung bestehen. Die Beurteilung ist anhand der dargestellten acht Prüfpunkte vorzunehmen, wobei die in der Rechtsprechung entwickelten Anforderungen nicht in jedem Fall kumulativ erfüllt sein müssen. Im Rahmen eines Prüfpunktes festgestellte Mängel können grundsätzlich durch andere Vorkehren zum Schutz vor Missbrauch ausgeglichen beziehungsweise kompensiert werden. Der Gerichtshof ist der Ansicht, dass der Prozess einer Massenüberwachung durchgehenden Garantien zum Schutz vor Missbrauch unterworfen werden muss. Er bezeichnet (entsprechend) die folgenden Aspekte als grundlegende Garantien zum Schutz vor Missbrauch, «qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8» (zit. Urteil Centrum för rättvisa, § 264): - Vorgängige unabhängige Genehmigung einer

Massenüberwachung (Prüfpunkt 3) - Durchgehende Beaufsichtigung durch eine unabhängige Behörde (Prüfpunkt 7) - Wirksames Rechtsmittel zur nachträglichen Überprüfung einer Überwachung (Prüfpunkt 8) Entsprechend ist auch hier vorzugehen. Es sind zunächst je Prüfpunkt die Ergebnisse der Beurteilung darzulegen (nachfolgend E. 25.2). Gestützt darauf ist sodann zu beurteilen, ob festgestellte Mängel durch andere Vorkehren zum Schutz vor Missbrauch ausgeglichen werden können (nachfolgend E. 25.3). Für den Fall, dass das anwendbare Recht insgesamt keine hinreichenden Vorkehren zum Schutz vor Missbrauch vorsieht und die Grundrechtsbeeinträchtigungen nicht gerechtfertigt werden können, ist entsprechend dem Unterlassungsbegehren der Beschwerdeführenden über die rechtlichen Folgen dieser Erkenntnis zu entscheiden (nachfolgend E. 25.4). Im Hinblick auf die nachfolgende Gesamtbeurteilung ist in Übereinstimmung mit der Rechtsprechung der Grossen Kammer des EGMR zu beachten, dass die Schwere der Beeinträchtigung des Privatlebens und der Medienfreiheit im Verlaufe des Prozesses der Massenüberwachung zunimmt und schliesslich besonders schwer wiegt (vgl. vorstehend E. 7.6.2). Besonders ins Gewicht fallen dabei die Anlasslosigkeit und die ausserordentliche Reichweite der Funk- und Kabelaufklärung. Im Weiteren anerkennt der EGMR, dass die Massenüberwachung der Telekommunikation von grosser Bedeutung ist, um Bedrohungen für die nationale Sicherheit frühzeitig zu erkennen. Für die Funk- und Kabelaufklärung ergibt sich Entsprechendes auch aus den bei den Akten liegenden Unterlagen. Es ist mithin davon auszugehen, dass es sich bei der Funk- und Kabelaufklärung um in der Praxis bedeutsame Mittel zur Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland handelt.

E. 25.2.1

Im Rahmen des ersten Prüfpunktes war zu untersuchen, ob das anwendbare Recht die Gründe, aus denen eine Funk- oder Kabelaufklärung eingesetzt werden darf, hinreichend bestimmt festlegt und ob damit die Beeinträchtigung der Grundrechte grundsätzlich gerechtfertigt werden kann. Gemäss dem anwendbaren Recht dient die Funk- und Kabelaufklärung der Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland, wobei mögliche Bedrohungen durch Terrorismus, die Verbreitung von Massenvernichtungswaffen oder für kritische Infrastrukturen nicht von vornherein feststehen, sich im Verlaufe der Zeit ändern und daher nicht generell-abstrakt festgeschrieben werden können. Die relative Offenheit des Gesetzes ist insoweit hinzunehmen, wobei nicht gesagt werden kann, die Gründe, aus denen die Funk- und Kabelaufklärung verwendet werden dürfen, blieben ohne ausreichend verbindliche Konturen. Soweit mit der relativen Offenheit des Gesetzes die Gefahr von Missbrauch verbunden ist, kann diese insbesondere durch die Pflicht einer vorgängigen Genehmigung durch eine unabhängige Behörde ausgeglichen werden (vgl. hierzu beim dritten Prüfpunkt). Bei den Gründen, aus denen eine Funk- oder Kabelaufklärung eingesetzt beziehungsweise genehmigt werden darf, handelt es sich zudem um zulässige Eingriffszwecke im Sinne von Art. 8 Ziff. 2 und Art. 10 Ziff. 2 EMRK. Die Beeinträchtigung der Grundrechte kann daher grundsätzlich und unter Vorbehalt der weiteren Prüfpunkte gerechtfertigt werden. Schliesslich ist in hinreichendem Mass vorhersehbar, dass die Funk- und Kabelaufklärung auch Vorgänge im Ausland mit einem Bezug zur Schweiz betreffen kann (sog. Schweiz-Bezug), wobei der Fokus eines Auftrags zur Aufklärung auf einem Vorgang im Ausland liegen muss (vgl. vorstehend E. 8 f., insbes. E. 9.4).

E. 25.2.2

Gemäss dem zweiten Prüfpunkt war zu beurteilen, ob die Umstände, unter denen die Kommunikation überwacht werden darf, hinreichend bestimmt im Gesetz festgelegt sind. Im Bereich der Massenüberwachung dürfen die Umstände weiter gefasst sein als bei einer gezielten Überwachung. Für die Kabelaufklärung sieht das anwendbare Recht vor, dass grenzüberschreitende Signale aus leitungsgebundenen Netzen erfasst werden dürfen. Rein schweizerische Kommunikationen, das heisst Kommunikationen, bei der sich Sender und Empfänger in der Schweiz befinden, dürfen nicht verwendet werden; können entsprechende Signale nicht bereits bei der Erfassung ausgeschieden werden, sind die entsprechenden Daten zu vernichten, sobald erkannt wird, dass es sich um rein schweizerische Kommunikation handelt. Die Rechtsprechung anerkennt sodann, dass bei der Erfassung von grenzüberschreitenden Signalen ein Ausscheiden von rein inländischer Kommunikation technisch nicht immer möglich ist. Dies ist hier jedoch nicht von entscheidender Bedeutung. Das Gesetz sieht eine Trennung von Informationsbeschaffung - durch den Beigeladenen - und nachrichtendienstlicher Auswertung und Verwendung - durch die Vorinstanz - vor. Zusammen mit dem erwähnten Verwendungsverbot besteht somit in hinreichendem Mass Gewähr dafür, dass rein schweizerische Kommunikation, selbst wenn sie nicht bereits bei der Erfassung ausgeschieden werden kann, nicht an die Vorinstanz weitergeleitet und von dieser verwendet wird. Die Umstände, unter denen die Kommunikation im Rahmen einer Kabelaufklärung überwacht werden darf, lassen sich sodann kaum weiter eingrenzen als in Bezug auf das Ziel der Überwachung. Die Umstände sind daher hier hinreichend vorhersehbar, wobei insbesondere das Verwendungsverbot für rein schweizerische Kommunikation und die Trennung von Informationsbeschaffung und nachrichtendienstlicher Auswertung in zweckmässiger Weise Schutz vor Missbrauch bieten (vgl. vorstehend E. 10 f, insbes. E. 11.4). Die Umstände, unter denen die Kommunikation überwacht werden darf, sind auch in Bezug auf die Funkaufklärung in hinreichendem Mass vorhersehbar; es können Funksignale aufgefangen werden, die von Telekommunikationssatteliten und Kurzwellensendern auch auf das Gebiet der Schweiz abgestrahlt werden (vgl. vorstehend E. 12).

E. 25.2.3

Im Rahmen des dritten Prüfpunktes war zu untersuchen, ob die Funk- und Kabelaufklärung ex ante einer Genehmigung durch eine unabhängige Behörde unterworfen sind und die Behörde über die hierfür erforderlichen Kenntnisse und Befugnisse verfügt, wobei nach der Rechtsprechung der Grossen Kammer des EGMR eine richterliche Genehmigung eine wichtige Garantie gegen Willkür ist, aber kein notwendiges Erfordernis darstellt. Weitere Beurteilungskriterien waren die Verbindlichkeit der Entscheidung der Behörde, die Festlegung der Suchbegriffe (nach Kategorien) und die zeitliche Befristung der Genehmigung. Die Untersuchung ergab, dass Aufträge zur Kabelaufklärung einem Genehmigungsvorbehalt unterworfen sind und für die Genehmigung mit dem Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) ein unabhängiges Gericht verantwortlich ist. Das Gericht verfügt zudem über die für eine Beurteilung notwendigen Informationen (Orientierung und Bedürfnis; Kategorien von Suchbegriffen [sog. Selektoren]; Angaben zu betroffenen Leitungen) und seine Entscheide sind verbindlich. Die Genehmigung ist ferner zeitlich befristet, wobei die Möglichkeit einer Verlängerung der Genehmigung besteht. Einem Gesuch um Verlängerung sind schliesslich die bisher gewonnenen Erkenntnisse beizulegen. Diese werden vom Bundesverwaltungsgericht (Abteilung I, Fachgebiet NDG) vorfrageweise auf ihre Rechtmässigkeit hin überprüft. Das anwendbare Recht bietet insoweit grundsätzlich in hinreichendem Mass Schutz vor

Missbrauch. Die Einschränkung an Transparenz beziehungsweise Öffentlichkeit - die Genehmigungsentscheide werden nicht veröffentlicht - ist dabei mit Blick auf das zwingende Erfordernis der Geheimhaltung hinzunehmen. Das für die Vorinstanz und den Beigeladenen geltende Recht enthält jedoch keine Regelung in Bezug auf die Verwendung sogenannter starker, das heisst personenbezogener Selektoren. Zwar sind Angaben über schweizerische natürliche und juristische Personen als Suchbegriffe nicht zulässig (Art. 39 Abs. 3 Satz 3 NDG), Angaben über Personen im Ausland und damit insbesondere auch zu Journalisten oder etwa Rechtsanwälten dürfen hingegen als Suchbegriffe verwendet werden. Werden wie hier im Rahmen der Genehmigung nur die Kategorien von Suchbegriffen genehmigt, verlangt die Grosse Kammer des EGMR zum Ausgleich der widerstreitenden Interessen, dass die Verwendung starker Selektoren einem Verfahren vorheriger (interner) Genehmigung unterworfen wird; die Verwendung von Suchbegriffen, von denen bekannt ist, dass sie mit einem Journalisten in Verbindung stehen, muss nach der Rechtsprechung des EGMR in jedem Fall von einem unabhängigen Entscheidungsgremium genehmigt werden. Das Fehlen einer Regelung, welche die vorherige Genehmigung starker Selektoren verbindlich vorschreibt, stellt einen Mangel im Verfahren dar. Dieser fällt insbesondere mit Blick auf besonders schützenswerte Kommunikationen ins Gewicht (vgl. vorstehend E. 14.4.2). Für Aufträge zur Funkaufklärung schreibt das anwendbare Recht keine unabhängige Genehmigung ex ante vor; Aufträge zur Funkaufklärung werden von der Vorinstanz im Rahmen der gesetzlichen Vorgaben in eigener Verantwortung erteilt. Dies stellt mit Blick auf die ebenfalls fehlende zeitliche Beschränkung einen grundlegenden Mangel im Verfahren dar (vgl. zum Ganzen vorstehend E. 13 f.).

E. 25.2.4

Im Rahmen des vierten Prüfpunktes waren die gesetzlichen Bestimmungen zur Auswahl, Auswertung und Verwendung der erfassten Telekommunikationen zu untersuchen. Beurteilungskriterien hierbei waren entsprechend der Rechtsprechung der Grossen Kammer des EGMR die Unterscheidung von inländischer und ausländischer Kommunikation, die Vorgaben für die Auswertung der erfassten Kommunikationen, die Vorhersehbarkeit der Datenbearbeitung, deren Protokollierung sowie der Schutz vertraulicher Kommunikationen. Die Untersuchung ergab, dass nach dem anwendbaren Recht die Verwendung von rein inländischer Kommunikation im Rahmen der Kabelaufklärung untersagt und Informationen über Personen im Inland der Vorinstanz grundsätzlich nur anonymisiert bekannt gegeben werden dürfen. Die betreffenden Vorgaben beschränken das Ermessen der Behörden und bieten insoweit grundsätzlich Schutz vor Missbrauch. Die Pflicht, Informationen über Personen im Inland nur anonymisiert an die Vorinstanz weiterzuleiten, gilt jedoch nicht absolut. Enthalten die Daten Informationen über Vorgänge im In- oder Ausland, die auf eine konkrete Bedrohung der inneren Sicherheit hinweisen, besteht die Möglichkeit einer sogenannten Entanonymisierung. Die Entanonymisierung steht nicht unter dem Vorbehalt einer Beurteilung durch eine unabhängige Behörde. Somit besteht insbesondere bei Resultaten mit einem Schweiz-Bezug die Gefahr, dass die Funk- und Kabelaufklärung für die Inlandsaufklärung missbraucht werden. Erkenntnisse aus der Funk- und Kabelaufklärung dürfen sodann den Strafverfolgungsbehörden bekannt gegeben werden, wiederum ohne, dass diesbezüglich eine verfahrensmässige Sicherung vorhanden wäre; weder steht die Bekanntgabe in formeller Hinsicht unter dem Vorbehalt einer Genehmigung durch eine unabhängige Behörde, noch schreibt das anwendbare Recht in materieller Hinsicht eine Interessenabwägung vor. Die Pflicht, Informationen über Personen im Inland unter Umständen unverändert an die Vorinstanz weiterzuleiten, birgt somit ein

Missbrauchspotential; es besteht etwa die Gefahr, dass Personen im Inland als Folge der Funk- und Kabelaufklärung zum Gegenstand weiterer behördlicher Massnahmen werden. Das anwendbare Recht bietet daher nicht in hinreichendem Mass Schutz vor Missbrauch und erweist sich als mangelhaft (vgl. vorstehend E. 16.3.2.2, 16.3.3 und 16.3.4.3). Als problematisch ist auch zu beurteilen, dass (vom Beigeladenen) nicht verlangt wird, die Methoden zur Aussonderung rein schweizerischer Kommunikation kontinuierlich weiterzuentwickeln (vgl. vorstehend E. 16.3.2.3). In der Praxis besteht weiter die Möglichkeit der sogenannten Retrosuche. Erfasste Kommunikationen können angesichts dessen, dass diese über einen längeren Zeitraum - bis zu fünf Jahren - aufbewahrt werden dürfen, zu einem späteren Zeitpunkt erneut durchsucht werden. Dabei können auch neu definierte Selektoren zur Anwendung gelangen. Es erscheint äusserst fraglich, ob die Möglichkeit der Retrosuche hinreichend vorhersehbar ist (vgl. vorstehend E. 16.3.4.4). Die Vorinstanz legt Resultate aus der Funk- und Kabelaufklärung in ihren Informationssystemen ab, ohne dass die betreffenden Originaldokumente auf ihre Richtigkeit und Erheblichkeit hin überprüft werden. Die Praxis der Vorinstanz bietet daher keine hinreichende Gewähr dafür, dass im Zusammenhang mit der Funk- und Kabelaufklärung nur richtige und erhebliche Daten bearbeitet werden (vgl. vorstehend E. 16.3.4.2). Ferner sind weder der Beigeladene noch die Vorinstanz verpflichtet, die Massenüberwachung über alle Schritte hinweg zu protokollieren und aufzuzeichnen, um eine (nachträgliche) Überprüfung zu ermöglichen (vgl. vorstehend E. 16.3.4.2 und E. 16.3.5). Besonders ins Gewicht fällt schliesslich, dass das anwendbare Recht keine Vorkehren beziehungsweise verfahrensrechtlichen Sicherungen zum Schutz journalistischer Quellen und anderer besonders schützenswerter Kommunikation wie etwa jener zwischen einem Rechtsanwalt und seinem Mandanten enthält. So steht etwa die Verwendung besonders schützenswerter Kommunikationen nicht unter dem Vorbehalt einer Beurteilung beziehungsweise Interessenabwägung durch eine unabhängige Behörde (vgl. vorstehend E. 16.3.6). Das für die Auswahl, Auswertung und Verwendung anwendbare Recht weist mithin verschiedene (grundlegende) Mängel (vgl. zum Ganzen vorstehend E. 15 f.).

E. 25.2.5

Im Rahmen des fünften Prüfpunktes war zu untersuchen, ob das anwendbare Recht im Zusammenhang mit der Bekanntgabe von Erkenntnissen aus der Funk- und Kabelaufklärung an andere Parteien in hinreichendem Mass Schutz vor Missbrauch bietet. Nach der Rechtsprechung der Grossen Kammer des EGMR ist erforderlich, dass die Übermittlung auf rechtmässig erhobene Daten und auf das Notwendig beschränkt ist, im Empfängerstaat ein angemessener Datenschutz gewährleistet ist, Vorkehren zum Schutz von vertraulichen Kommunikationen bestehen und die Übermittlung einer unabhängigen Kontrolle unterliegt. Die Untersuchung ergab, dass die Bekanntgabe von Erkenntnissen an Behörden im Inland auf das Notwendig und damit in hinreichendem Mass eingeschränkt ist; die Möglichkeit der Bekanntgabe von Informationen an die Strafverfolgungsbehörde ist im Zusammenhang mit der Entanonymisierung von Daten im Rahmen des vierten Prüfpunktes beurteilt worden. Die Bekanntgabe von Erkenntnissen an ausländische Behörden ist sodann nur zulässig, wenn der Empfängerstaat einen angemessenen Datenschutz gewährleistet. Das anwendbare Recht enthält jedoch keinen hinreichend verbindlichen Massstab zur Beurteilung besagter Angemessenheit, ohne dass dieser Mangel allzu schwer wiegen würde. Anders ist der Umstand zu beurteilen, dass das anwendbare Recht keine besonderen Garantien vorsieht, wenn etwa journalistisches Material übermittelt werden soll. Dieser Mangel wiegt schwer. Schliesslich fehlt es an einer unabhängigen Kontrolle, die zumindest

stichprobenweise einzelne Datenbearbeitungen überprüft (vgl. zum Ganzen vorstehend E. 17, insbes. E. 17.3).

E. 25.2.6

Gemäss dem sechsten Prüfpunkt war zu beurteilen, ob das anwendbare Recht hinsichtlich der Dauer einer Überwachung und der Aufbewahrung von Daten hinreichende Garantien zum Schutz vor Missbrauch enthält. Nach der Rechtsprechung der Grossen Kammer des EGMR ist es erforderlich, dass die Überwachung zeitlich begrenzt ist, die Umstände, unter denen eine Überwachung beendet werden muss, festgelegt sind, die Aufbewahrung der Daten zeitlich begrenzt ist und damit verbunden eine Pflicht zur Löschung von Daten besteht. Die Untersuchung ergab, dass das anwendbare Recht die Dauer der Kabelaufklärung hinreichend vorhersehbar und in angemessener Weise begrenzt. Nicht mit der erforderlichen Bestimmtheit vorgeschrieben ist hingegen, dass eine Kabelaufklärung vorzeitig zu beenden ist, wenn die Voraussetzungen für ihre Durchführung nicht mehr gegeben sind. Dasselbe gilt für die Funkaufklärung, wobei deren Dauer durch das anwendbare Recht in keiner Weise begrenzt wird. Diese Mängel wiegen nicht leicht. Die Resultate aus der Funk- und Kabelaufklärung werden von der Vorinstanz sodann insbesondere im integralen Analysesystem (IASA NDB) abgelegt und bearbeitet. Wie sich diesbezüglich die Aufbewahrungsfrist konkret berechnet, ist auch gestützt auf die Erläuterungen der Vorinstanz nicht nachvollziehbar und damit nicht in hinreichendem Mass vorhersehbar. Zudem kommt die Dauer der Aufbewahrung und damit der Bearbeitung einer unbefristeten und damit unzulässigen Aufbewahrung im Sinne der Rechtsprechung des EGMR zumindest sehr nahe; im integralen Analysesystem (IASA NDB) dürfen Daten bis zu 45 Jahre lang aufbewahrt werden. Immerhin bietet die Praxis von Beigeladenem und Vorinstanz ausreichend Gewähr dafür, dass Daten nach Ablauf der zulässigen Aufbewahrungsfristen gelöscht werden. Insgesamt bietet das anwendbare Recht in Bezug auf die Dauer der Aufbewahrung von Resultaten aus der Funk- und Kabelaufklärung durch die Vorinstanz jedoch keinen hinreichenden Schutz vor Missbrauch (vgl. zum Ganzen vorstehend E. 18, insbes. E. 18.3).

E. 25.2.7

Im Rahmen des siebten Prüfpunktes war zu untersuchen, ob jede Phase der Massenüberwachung der Beaufsichtigung durch eine unabhängige Behörde unterworfen ist, die über die Befugnisse verfügt, um die Überwachung und die Beeinträchtigung des Privatlebens und der Medienfreiheit auf das Notwendige zu beschränken. Im Vordergrund steht hier die unabhängige Kontrollinstanz für die Funk- und Kabelaufklärung UKI. Dabei handelt es sich um eine unabhängige Behörde, die grundsätzlich den gesamten Prozess der Informationsbeschaffung überwacht. Zudem überprüft sie alle Funkaufklärungsaufträge auf ihre Rechtmässigkeit hin. Die Kontrollinstanz hat Zugang zu allen zweckdienlichen Informationen und Anlagen und führt jährlich insgesamt fünf eintägige Inspektionsbesuche bei der Vorinstanz und dem Beigeladenen durch. Hierbei überprüft sie insbesondere die Rechtmässigkeit von Resultaten aus der Funk- und Kabelaufklärung, wobei die Überprüfung stichprobenweise erfolgt. In diesem Rahmen ist die Kontrollinstanz nicht in der Lage, fortlaufend eine bedeutende Anzahl von Resultaten aus der Funk- und Kabelaufklärung auf ihre Rechtmässigkeit hin zu überprüfen. Zudem sind die Berichte über ihre Prüfungen nicht öffentlich zugänglich, obschon eine Veröffentlichung in geeigneter Form, das heisst beispielswiese mit Schwärzungen oder in zusammengefasster Form, möglich wäre. Die tatsächliche Aufsichtstätigkeit der unabhängigen Kontrollinstanz für die

Funk- und Kabelaufklärung UKI im Bereich der Informationsbeschaffung bietet insoweit keinen fortlaufenden und effektiven und damit keinen hinreichenden Schutz vor Missbrauch (vgl. hierzu vorstehend E. 21.2.2). Dasselbe ergab sich für die Tätigkeit der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND und der Geschäftsprüfungsdelegation GPDel, die nur - aber immerhin - auf das Erkennen systematischer Probleme ausgerichtet sind. Auch die Datenbearbeitung durch die Vorinstanz untersteht somit keiner hinreichend effektiven Beaufsichtigung. Diese Mängel wiegen mit mit Blick auf die Gewichtung, welche der EGMR einer unabhängigen Kontrolle beigibt, schwer (vgl. zum Ganzen vorstehend E. 19-21, insbes. E. 21).

E. 25.2.8

Schliesslich war im Rahmen des achten Prüfpunktes zu untersuchen, ob das anwendbare Recht eine effektive nachträgliche Überprüfung ermöglicht. Nach der Rechtsprechung der Grossen Kammer des EGMR zur Massenüberwachung muss die nachträgliche Überprüfung durch eine unabhängige Behörde erfolgen. Weitere Beurteilungskriterien waren die Zuständigkeit und die Befugnisse der Behörde sowie die Ausgestaltung des Verfahrens. Die Untersuchung ergab, dass Rechtsschutz im Rahmen der Funk- und Kabelaufklärung nicht ausgeschlossen ist. Zwar kann das datenschutzrechtliche Auskunftsrecht, das zu Beginn der nachträglichen Prüfung steht, beispielsweise durch einen Aufschub der Auskunft eingeschränkt werden. Fehlt es an einem Geheimhaltungsinteresse oder fällt dieses weg, ist jedoch nach den Bestimmungen des DSG Auskunft zu erteilen und es stehen dann auch die Ansprüche gemäss Art. 41 DSG offen. Der Aufschub der Auskunft ist im hier betroffenen Regelungsbereich grundsätzlich mit Art. 8 EMRK vereinbar, da mit dem indirekten Auskunftsrecht ein Mechanismus zur Verhinderung von Missbrauch zur Verfügung steht. Im Bereich der Funk- und Kabelaufklärung fällt jedoch in Betracht, dass die Aufbewahrung und damit grundsätzlich auch der Aufschub der Auskunft einer unbefristeten Auskunft zumindest sehr nahe kommt. Es kann daher nicht gesagt werden, es bestehe im Falle eines Aufschubs der Auskunft bereits heute effektiver Rechtsschutz, sobald die Geheimhaltungsinteressen weggefallen sind und alsdann Auskunft erteilt wird (vgl. hierzu vorstehend E. 24.2.1). Auch das indirekte Auskunftsrecht ermöglicht keine nachträgliche Überprüfung im Sinne der Rechtsprechung der Grossen Kammer des EGMR zur Massenüberwachung. Zwar steht dieses jeder Person zu und es wird mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB von einer unabhängigen Behörde bearbeitet, die Überprüfung erfolgt jedoch weder in einem kontradiktorischen Verfahren unter Gewährung von Parteirechten (vgl. zur Prozessvertretung im englischen Recht vorstehend E. 22.2.1), noch erhält die gesuchstellende Person inhaltlich Auskunft (vgl. hierzu vorstehend E. 24.2.2). In Betracht fiel zudem, dass auch das Datenschutzrecht den Aufschub beziehungsweise die Verweigerung einer Auskunft aufgrund überwiegender Geheimhaltungsinteressen zulässt. Im Unterscheid zur indirekten Auskunft ergeht der Entscheid gestützt auf das Datenschutzgesetz jedoch in einem kontradiktorischen Verfahren und die Behörde erlässt eine Verfügung, gegen die der ordentliche Rechtsmittelweg - hier an das Bundesverwaltungsgericht - offen steht. Zwar wird auch in einem solchen Verfahren im Falle überwiegender Geheimhaltungsinteressen weder Akteneinsicht gewährt noch unmittelbar Auskunft erteilt. Der Entscheid ergeht jedoch in einem ordentlichen (Rechtsmittel-)Verfahren unter Gewährung von Parteireichten durch ein Gericht mit umfassenden Befugnissen (vgl. hierzu vorstehend E. 24.2.3). Vor diesem Hintergrund kann nicht gesagt werden, dass das anwendbare Recht, das einen Aufschub der Auskunft und das

indirekte Auskunftsrecht vorsieht, eine effektive nachträgliche Überprüfung ermöglicht. Es erweist sich insoweit als mangelhaft (vgl. zum Ganzen vorstehend E. 22-24).

E. 25.3

Mit dem EGMR ist davon auszugehen, dass die Funk- und Kabelaufklärung als Mittel zur Massenüberwachung ein beträchtliches Missbrauchspotential aufweisen. Die vermutete Bearbeitung von Daten der Beschwerdeführenden kann daher nur konform sein mit den durch Bundesverfassung und EMRK geschützten Rechten, wenn das anwendbare Recht insgesamt in hinreichendem Mass Schutz vor Missbrauch bietet. Vorliegend sind die Gründe und die Umstände, unter denen die Kommunikation im Rahmen einer Funk- oder Kabelaufklärung überwacht werden darf, grundsätzlich hinreichend vorhersehbar im Gesetz festgelegt. Zudem ist vorhersehbar, dass die Funk- und Kabelaufklärung auch Vorgänge im Ausland mit einem Bezug zur Schweiz betreffen kann. Für die Kabelaufklärung ist sodann vorgeschrieben, dass rein schweizerische Kommunikation nicht verwendet werden darf. Kann der Beigeladene solche Signale nicht bereits bei der Erfassung ausscheiden, so sind die betreffenden Daten zu vernichten, sobald erkannt wird, dass es sich um rein schweizerische Kommunikation handelt. Hierbei und im Allgemeinen ist auch die organisatorische Trennung von Informationsbeschaffung durch den Beigeladenen und nachrichtendienstlicher Auswertung durch die Vorinstanz von besonderer Bedeutung. Selbst wenn mithin rein schweizerische Kommunikation nicht bereits bei der Erfassung erkannt wird, bietet die organisatorische Trennung (zusätzlich) Gewähr dafür, dass rein schweizerische Kommunikation nicht durch den Nachrichtendienst ausgewertet und verwendet wird. Aufträge zur Kabelaufklärung stehen im Weiteren unter dem Genehmigungsvorbehalt durch ein unabhängiges Gericht. Für die Genehmigung ex ante zuständig ist das Bundesverwaltungsgericht. Dessen Entscheide sind verbindlich und befristet, wobei die Möglichkeit einer Verlängerung der Genehmigung besteht. Das Bundesverwaltungsgericht überprüft im Rahmen eines Gesuchs um Verlängerung der Genehmigung sodann vorfrageweise die Rechtmässigkeit der bisher erzielten Resultate. Zwar ist das Genehmigungsverfahren nicht öffentlich und das anwendbare Recht sieht zum Ausgleich der berührten Interessen auch keine Teilnahme eines Datenschutzbeauftragten am Verfahren vor. Der Genehmigungsvorbehalt ist unter Berücksichtigung der diesbezüglichen Praxis des Bundesverwaltungsgerichts jedoch eine taugliche und wichtige Garantie zum Schutz vor Missbrauch. Zudem können hierdurch andere Mängel im Verfahren, wie etwa die fehlenden Genehmigungsvorbehalte bei der Verwendung starker Selektoren und bei der Entanonymisierung von Informationen über Personen im Inland wenn auch nicht beseitigt, so doch immerhin gemildert werden. Insgesamt vermag das anwendbare Recht unter Berücksichtigung der tatsächlichen Funktionsweise der Funk- und Kabelaufklärung nicht in hinreichendem Mass Schutz vor Missbrauch zu bieten. Dabei fällt mit Blick auf die Rechtsprechung der Grossen Kammer des EGMR besonders ins Gewicht, dass die Funkaufklärung weder einer Genehmigungspflicht noch einer zeitlichen Befristung unterworfen ist. Zudem ist nicht gewährleistet, dass die Vorinstanz nur erhebliche und richtige Daten bearbeitet. Das anwendbare Recht enthält sodann keine Vorkehren zum Schutz journalistischer Quellen und von anderen besonders schützenswerten Kommunikationen; es besteht weder bei der Erfassung noch bei der Bearbeitung und der Weiterleitung eine Pflicht zur Aussonderung oder Vernichtung beziehungsweise ein Vorbehalt vor der weiteren Bearbeitung. Schliesslich ist durch die Tätigkeiten der unabhängigen Kontrollinstanz für die Funk- und Kabelaufklärung UKI und der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND

weder eine hinreichend effektive Beaufsichtigung der Informationsbeschaffung durch die Funk- und Kabelaufklärung gewährleistet, noch steht Betroffenen wie den Beschwerdeführenden ein wirksames Rechtsmittel für eine nachträgliche Überprüfung zur Verfügung. Die nachträgliche Kontrolle und Überprüfung werden zudem dadurch erschwert, dass der Beigeladene und die Vorinstanz nicht verpflichtet sind, die Überwachung über alle Schritte hinweg zu protokollieren. Eine fortlaufende und effektive Überwachung der Massenüberwachungen durch eine unabhängige Kontrollinstanz ist damit nicht gewährleistet. Unter diesen Umständen können andere Mängel im Verfahren wie etwa die fehlende Genehmigungspflicht für starke Selektoren, die nicht hinreichend bestimmte Pflicht zur vorzeitigen Beendigung einer Kabelaufklärung bei Wegfall von deren Voraussetzungen, der fehlende Schutz in Bezug auf die Weiterleitung von Informationen über Personen im Inland an die Vorinstanz oder die unzureichende Begrenzung der Dauer der Aufbewahrung von Daten durch die Vorinstanz nicht ausgeglichen beziehungsweise gemindert werden. Die Beeinträchtigung der Grund- und Konventionsrechte der Beschwerdeführenden kann nach dem Gesagten nicht gerechtfertigt werden. Im Gesamtergebnis verletzt die Vorinstanz mit der Beschaffung von Informationen durch die Funk- und Kabelaufklärung und damit der vermuteten Bearbeitung von Daten der Beschwerdeführenden deren Anspruch auf Achtung des Privatlebens (Art. 8 EMRK, Art. 13 BV) und der Medienfreiheit (Art. 10 EMRK, Art. 17 BV).

E. 25.4

Zu prüfen ist, welche Rechtsfolgen sich aus der Verletzung der Grundrechte der Beschwerdeführenden ergeben. Das Bundesgericht hielt in seinem Rückweisungsentscheid fest (Rückweisungsentscheid 1C_377/2019 vom 1. Dezember 2020 E. 10.1 [Hervorhebungen nur hier]): Mit den Begehren 1 und 2 wird die Unterlassung der Funk- und Kabelaufklärung verlangt (Art. 25 Abs. 1 lit. a [a]DSG). Grundsätzlich beschränkt sich das schutzwürdige Interesse der Beschwerdeführenden auf den Schutz ihrer eigenen Daten und allenfalls (für die Beschwerdeführenden 4-6 und 8) der Daten ihrer Quellen und ihrer Klientschaft [...]. Allerdings stellt sich die Frage, ob es technisch möglich ist, die Daten einzelner Personen von der Funk- und Kabelaufklärung auszunehmen. Dies erscheint zweifelhaft, aufgrund der grossen Menge an ausgeleiteten und durchsuchten Daten und der Tatsache, dass diese erst in einer späten Phase bestimmten Personen zugeordnet werden. Es kann daher nicht von vornherein ausgeschlossen werden, dass die Einstellung der Funk- und Kabelaufklärung das einzige Mittel sein könnte, um einen wirksamen Grundrechtsschutz für die Beschwerdeführenden sicherzustellen. Unter diesen Umständen ist auf die Begehren 1 und 2 einzutreten; es wird Sache der materiellen Beurteilung sein, ob und inwieweit die Unterlassungsansprüche begründet sind. Ergibt sich wie hier, dass eine Datenbearbeitung nicht mit den Grund- und Konventionsrechten der Beschwerdeführenden vereinbar und damit widerrechtlich ist, hat die Bearbeitung grundsätzlich zu unterbleiben (Art. 6 Abs. 1 und Art. 41 Abs. 1 Bst. a DSG). Der Anspruch der Beschwerdeführenden auf Unterlassung beschränkt sich dabei, dem schutzwürdigen Interesse entsprechend, auf die Bearbeitung der eigenen Personendaten und allenfalls der Daten ihrer Quellen und ihrer Klientschaft. Soweit es jedoch technisch nicht möglich ist, die Daten einzelner Personen von der Überwachung (Funk- und Kabelaufklärung) auszunehmen, impliziert der eben zitierte Rückweisungsentscheid als letztes Mittel deren Einstellung. Die Funk- und Kabelaufklärung sind keine Mittel zur Überwachung der Kommunikation bestimmter Personen (im Inland) und Angaben über schweizerische natürliche oder juristische Personen sind als Suchbegriffe jedenfalls im Rahmen der Kabelaufklärung nicht zulässig

(Art. 39 Abs. 3 NDG). Es liegt jedoch in der Natur der Funk- und Kabelaufklärung, dass sie im Vergleich zur Überwachung der individuellen Kommunikation weniger zielgenau ist und generell die grenzüberschreitende Kommunikation zum Gegenstand hat. Zudem bringen der Beigeladene und die Vorinstanz nicht vor und es ist auch nicht ohne Weiteres ersichtlich, dass es technisch möglich ist, die Daten einzelner Personen bereits von der Erfassung durch den Beigeladenen auszunehmen. Unter diesen Umständen hat die festgestellte Verletzung der Grund- und Konventionsrechte der Beschwerdeführenden entsprechend dem Rückweisungsentscheid des Bundesgerichts zur Folge, dass die Funk- und Kabelaufklärung so, wie sie derzeit praktiziert wird, einzustellen ist. Bei diesem Ergebnis ist indessen zu berücksichtigen was folgt: Das NDG soll gestützt auf Empfehlungen und Vorschläge der Geschäftsprüfungsdelegation GPDel revidiert werden; die Vernehmlassung zur geplanten Gesetzesrevision fand bereits statt (vgl. vorstehend E. 4.3). Vor diesem Hintergrund und mit Blick auf die praktische Bedeutung der Funk- und Kabelaufklärung für die Informationsbeschaffung rechtfertigt es sich nicht, die Einstellung der Funk- und Kabelaufklärung unmittelbar anzuordnen. Zudem ist festzuhalten, dass die Funk- und Kabelaufklärung nicht als von vornherein mit der Bundesverfassung und der EMRK unvereinbar erscheinen. Die Mängel sind vielmehr bekannt und können, wie die vorstehenden Erwägungen gezeigt haben, grundsätzlich behoben werden. Aus diesen Gründen ist dem Gesetzgeber die Gelegenheit zu geben, in Bezug auf die Funk- und Kabelaufklärung einen insgesamt mit der Bundesverfassung und der EMRK konformen Zustand herzustellen. Hierfür erscheint unter Berücksichtigung der gesamten Umstände (insbesondere Bedeutung der Funk- und Kabelaufklärung, Verletzung der Grundrechte der Beschwerdeführenden, Berücksichtigung des demokratischen Prozesses) eine Frist von fünf Jahren ab Rechtskraft des vorliegenden Urteils als angemessen. Die Beschwerde ist daher in diesem Sinne gutzuheissen. Sollte innerhalb dieser Frist kein mit der Bundesverfassung und der EMRK konformer Zustand im Sinne der Rechtsprechung der Grossen Kammer des EGMR zur Massenüberwachung sowie des vorliegenden Urteils hergestellt worden sein, sind die Funk- und die Kabelaufklärung nach Massgabe des bundesgerichtlichen Rückweisungsentscheids einzustellen beziehungsweise zu unterlassen. Bei diesem Ergebnis ist auf die Feststellungsbegehren der Beschwerdeführenden, die gemäss dem Rückweisungsentscheid als Eventualanträge entgegenzunehmen sind, nicht weiter einzugehen. Beweisanträge

E. 26

Die Beschwerdeführenden stellen verschiedene Beweisanträge. Sie beantragen insbesondere, es seien verschiedene Personen zur Sache und insbesondere zur Funktionsweise des Internets sowie zu den Möglichkeiten der Aussonderung rein inländischer Kommunikation zu befragen beziehungsweise es seien (im Rahmen eines Gutachtens) Experten zur Beantwortung dieser Fragen beizuziehen. Mit Blick auf das Ergebnis des Beschwerdeverfahrens und unter Verweis auf die Erwägungen insbesondere zu den Möglichkeiten und Grenzen der Aussonderung rein schweizerischer Kommunikation (vgl. vorstehend E. 11.4) besteht kein begründeter Anlass, die von den Beschwerdeführenden genannten Personen zu befragen oder bestimmte Personen (im Rahmen von Gutachten) als Experten beizuziehen. Die Beweisanträge der Beschwerdeführenden sind in antizipierter Beweiswürdigung (BGE 141 I 60 E. 3.3) abzuweisen. Aus dem gleichen Grund ist auch auf die Beweisofferte der Vorinstanz nicht weiter einzugehen. Kostenentscheid

E. 27.1

Es bleibt, über die Kosten- und Entschädigungsfolgen für das vorliegende Beschwerdeverfahren (erster und zweiter Rechtsgang) zu entscheiden.

E. 27.2

Das Bundesverwaltungsgericht auferlegt die Kosten für das Beschwerdeverfahren in der Regel der unterliegenden Partei. Ausnahmsweise können die Kosten erlassen werden (Art. 63 Abs. 1 VwVG). Keine Verfahrenskosten werden Vorinstanzen oder beschwerdeführenden und unterliegenden Bundesbehörden auferlegt (Art. 63 Abs. 2 VwVG). Die Beschwerdeführenden sind vorliegend als obsiegend anzusehen. Es sind ihnen daher keine Verfahrenskosten aufzuerlegen und der von den Beschwerdeführenden in der Höhe von Fr. 2'000.- geleistete Kostenvorschuss ist ihnen nach Eintritt der Rechtskraft des vorliegenden Urteils zurückzuerstatten. Ebenfalls keine Verfahrenskosten tragen die Vorinstanz und der Beigeladene. Es sind daher keine Verfahrenskosten zu erheben.

E. 27.3

Das Bundesverwaltungsgericht spricht der ganz oder teilweise obsiegenden Partei von Amtes wegen oder auf Begehren eine Entschädigung für ihr erwachsene notwendige und verhältnismässig hohe Kosten zu (Art. 64 Abs. 1 VwVG). Die Parteientschädigung umfasst die Kosten der Vertretung sowie allfällige weitere Auslagen der Partei (Art. 8 Abs. 1 des Reglements über die Kosten und Entschädigungen vor dem Bundesverwaltungsgericht [VGKE, SR 173.320.2]). Das Bundesverwaltungsgericht legt die Höhe der Parteientschädigung aufgrund einer detaillierten Kostennote oder, wenn keine Kostennote beigebracht wird, aufgrund der Akten fest (Art. 14 VGKE). Die Entschädigung für die anwaltliche Vertretung wird nach dem zeitlichen Aufwand bemessen, wobei bei der Beurteilung des notwendigen und verhältnismässigen Aufwands nebst der Komplexität der Streitsache auch zu berücksichtigen ist, ob der Rechtsvertretung die Sach- und Rechtslage bereits bekannt war (vgl. Urteile des BGer 2C_730/2017 vom 4. April 2018 E. 3.5.2 und 8C_329/2011 vom 29. Juli 2011 E. 6). Die obsiegenden Beschwerdeführenden haben keine Kostennote eingereicht. Die Höhe der ihnen zuzusprechenden Parteientschädigung ist daher aufgrund der Akten zu bestimmen. Das Bundesverwaltungsgericht erachtet unter Berücksichtigung der beiden Rechtsgänge, der im Rahmen der verschiedenen Schriftenwechsel und als Antworten auf die Fragenkataloge des Bundesverwaltungsgerichts eingereichten Unterlagen sowie der Komplexität des Verfahrens eine Parteientschädigung in der Höhe von Fr. 18'000.- für angemessen. Diese ist den Beschwerdeführenden von der Vorinstanz nach Eintritt der Rechtskraft des vorliegenden Urteils zu bezahlen. Keinen Anspruch auf eine Parteientschädigung haben die Vorinstanz und der Beigeladene (Art. 7 Abs. 1 und 3 VGKE).