

Urteilkopf

147 I 280

21. Auszug aus dem Urteil der I. öffentlich-rechtlichen Abteilung i.S. Digitale Gesellschaft und Mitb. gegen Nachrichtendienst des Bundes NDB (Beschwerde in öffentlich-rechtlichen Angelegenheiten) 1C_377/2019 vom 1. Dezember 2020

Regeste (de):

Unterlassungs- und Feststellungsgesuche betreffend Funk- und Kabelaufklärung (Art. 38 ff. NDG); Anspruch auf materielle Beurteilung der Gesuche (Art. 25 Abs. 1 DSG; Art. 13 EMRK).

Bei der Funk- und Kabelaufklärung werden Personendaten bearbeitet, unabhängig davon, ob Informationen durch den NDB gespeichert werden (E. 6.1). Die Beschwerdeführenden sind potenziell in gleicher Weise von der Funk- und Kabelaufklärung betroffen wie alle Kommunikationsteilnehmer (E. 6.2.2). Speziell betroffen sind Medienschaffende sowie Anwälte und Anwältinnen (E. 6.2.3).

Das Recht auf wirksame Beschwerde gemäss Art. 13 EMRK kann bei geheimen Überwachungsmaßnahmen eingeschränkt oder aufgeschoben werden, wenn überwiegende Geheimhaltungsinteressen dies rechtfertigen und das System insgesamt mit Art. 8 EMRK vereinbar ist (E. 7.1). Dies muss von einer unabhängigen Instanz innerstaatlich überprüft werden können (E. 7.2). Für die "Opferstellung" i.S.v. Art. 34 EMRK genügt nach der EGMR-Rechtsprechung die hinreichende Wahrscheinlichkeit, einer geheimen Überwachung ausgesetzt zu sein, wenn es nicht möglich oder zumutbar ist, Beschwerde gegen konkrete Überwachungsmaßnahmen zu ergreifen (E. 7.2.2).

Die Beschwerdeführenden werden durch die Funk- und Kabelaufklärung mit hinreichender Wahrscheinlichkeit in ihrem Recht auf informationelle Selbstbestimmung (Art. 8 EMRK und Art. 13 BV) tangiert (E. 8). Sie haben keine Möglichkeit, Kenntnis von sie betreffenden Massnahmen der Funk- und Kabelaufklärung zu erhalten (E. 9.2) und sind daher darauf angewiesen, das System der Funk- und Kabelaufklärung in der Schweiz auf seine Verfassungs- und EMRK-Konformität überprüfen zu lassen. Dies stellt keine abstrakte Normenkontrolle dar: Gegenstand der Prüfung ist nicht das Gesetz als solches, sondern die (vermutete) Erfassung von Daten der Beschwerdeführenden (E. 9.3). Auf die Gesuche ist daher grundsätzlich nach Art. 25 Abs. 1 DSG i.V.m. Art. 13 EMRK einzutreten (E. 9.4).

Regeste (fr):

Action en cessation et en constatation portant sur l'exploration radio et du réseau câblé (art. 38 ss LRens); droit à un examen matériel des requêtes (art. 25 al. 1 LPD; art. 13 CEDH).

Lors de l'exploration radio et du réseau câblé, des données personnelles sont traitées, indépendamment de la question de savoir si les informations sont enregistrées par le Service de renseignement de la Confédération (SRC) (consid. 6.1). Les requérants sont potentiellement touchés de la même manière par l'exploration radio et du réseau câblé que tous les utilisateurs des télécommunications (consid. 6.2.2). Sont spécialement touchés les journalistes de même que les avocats et les avocates (consid. 6.2.3).

Le droit à un recours effectif au sens de l'art. 13 CEDH peut être limité ou différé lors de mesures de surveillance secrètes, si des intérêts prépondérants au maintien du secret le justifient et si le système est dans l'ensemble compatible avec l'art. 8 CEDH (consid. 7.1). Cela doit pouvoir être vérifié par une instance indépendante au niveau national (consid. 7.2). Pour admettre la "qualité de victime" au sens de l'art. 34 CEDH, il suffit, selon la jurisprudence de la CourEDH, de faire l'objet d'une surveillance secrète avec une vraisemblance suffisante, lorsqu'il n'est pas possible ou qu'il ne peut être exigé qu'un recours soit formé contre des mesures concrètes (consid. 7.2.2).

Les requérants sont affectés par l'exploration radio et du réseau câblé avec une vraisemblance suffisante dans leur droit à l'autodétermination informationnelle (art. 8 CEDH et art. 13 Cst.;

consid. 8). Ils n'ont pas la possibilité de prendre connaissance des mesures les concernant (consid. 9.2), de sorte qu'il est indispensable pour eux de pouvoir faire contrôler en Suisse la constitutionnalité et la conformité avec la CEDH du système de l'exploration radio et du réseau câblé. Cela ne constitue pas un contrôle abstrait des normes: l'objet de l'examen n'est pas la loi en tant que telle, mais la saisie (présumée) des données des recourants (consid. 9.3). Il convient en principe d'entrer en matière sur les requêtes selon l'art. 25 al. 1 LPD en relation avec l'art. 13 CEDH (consid. 9.4).

Regesto (it):

Richieste di cessazione e di accertamento relative a esplorazioni radio e di segnali via cavo (art. 38 segg. LAIn); diritto a un esame materiale delle domande (art. 25 cpv. 1 LPD; art. 13 CEDU).

Nell'ambito delle esplorazioni radio e di segnali via radio i dati personali vengono trattati, indipendentemente dal fatto che le informazioni siano memorizzate da parte del Servizio delle attività informative della Confederazione (consid. 6.1). I ricorrenti sono potenzialmente toccati dalle esplorazioni radio e di segnali radio alla stessa maniera degli altri utenti delle telecomunicazioni (consid. 6.2.2). Sono toccati in maniera particolare gli operatori dei media nonché gli avvocati e le avvocate (consid. 6.2.3).

Il diritto a un ricorso effettivo secondo l'art. 13 CEDU può essere limitato o differito nell'ambito di misure di sorveglianza segrete, qualora lo giustifichino prevalenti interessi di segretezza e il sistema sia complessivamente conforme all'art. 8 CEDU (consid. 7.1). Ciò deve poter essere verificato da un'istanza indipendente a livello nazionale (consid. 7.2). Per ammettere la "qualità di vittima" ai sensi dell'art. 34 CEDU, secondo la giurisprudenza della Corte EDU basta che sussista una probabilità sufficiente d'essere esposti a una sorveglianza segreta, qualora non sia possibile o non si possa ragionevolmente pretendere di presentare un ricorso contro misure di sorveglianza concrete (consid. 7.2.2).

I ricorrenti sono toccati nel loro diritto di autodeterminazione informativa con una probabilità sufficiente da esplorazioni radio e di segnali via cavo (art. 8 CEDU e art. 13 Cost.; consid. 8). Essi non hanno alcuna possibilità di venire a conoscenza delle misure di esplorazioni radio e di segnali via cavo che li concernono (consid. 9.2) e devono quindi poter fare esaminare la costituzionalità e la conformità alla CEDU del sistema svizzero di esplorazioni radio e di segnali via cavo. Ciò non costituisce un controllo astratto delle norme: oggetto dell'esame non è la legge in quanto tale, ma la (presunta) raccolta di dati dei ricorrenti (consid. 9.3). Occorre quindi di massima entrare nel merito delle richieste secondo l'art. 25 cpv. 1 LPD in relazione con l'art. 13 CEDU (consid. 9.4).

Sachverhalt ab Seite 282

BGE 147 I 280 S. 282

A. Der Verein Digitale Gesellschaft sowie die im Rubrum genannten Privatpersonen (nachfolgend: Gesuchstellende) wandten sich am 31. August 2017 an den Nachrichtendienst des Bundes (NDB) mit folgenden Begehren: "1. Der Betrieb der Funk- und Kabelaufklärung durch den NDB und weitere Stellen, namentlich durch das Zentrum für elektronische Operationen der Armee (ZEO), sowie jegliche Tätigkeiten, die dem Betrieb der Funkaufklärung und Kabelaufklärung dienen, seien zu unterlassen. 2. Der NDB habe jegliche in den Betrieb der Funk- und Kabelaufklärung involvierte Stellen und Personen anzuweisen, ihre diesbezügliche Tätigkeit zu unterlassen. 3. Es sei den GesuchstellerInnen mitzuteilen, ob und in welcher Weise Kommunikation von ihnen Gegenstand der Funk- oder Kabelaufklärung ist oder gewesen ist, und es sei ihnen mitzuteilen, welche sie betreffenden Daten, welche aus der Funk- oder Kabelaufklärung stammen, vom NDB oder vom ZEO bearbeitet werden, einschliesslich der Auskunft über weitere Daten, welche im Zusammenhang mit diesen aus der Funk- oder Kabelaufklärung stammenden Daten bearbeitet werden. 4. Es sei festzustellen, dass die Funk- und Kabelaufklärung die GesuchstellerInnen in ihren Grundrechten verletzt, namentlich ihrem Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor

Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]), in ihrer Freiheit der Meinungsäusserung, der Meinungs- und Informations- sowie die Medienfreiheit (Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Pakt II) und der Versammlungsfreiheit (Art. 22 BV, Art. 11 EMRK), in ihrer persönlichen Freiheit und der Bewegungsfreiheit (Art. 10 Abs. 2 BV, Art. 8 EMRK) sowie ihre Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV).

BGE 147 I 280 S. 283

5. Es sei festzustellen, dass die Funk- und Kabelaufklärung die Gesuch stellerInnen 4, 5 und 6 als JournalistInnen in ihrem Anspruch auf Medienfreiheit und auf Quellenschutz (Art. 17 BV und Art. 10 EMRK) verletzt. 6. Es sei festzustellen, dass die Funk- und Kabelaufklärung den Gesuchsteller 8 im Berufsgeheimnis als Rechtsanwalt und dadurch in seinem Recht auf Achtung des Privatlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]) und in seiner Wirtschaftsfreiheit (Art. 27 BV) verletzt; [...]" Der NDB antwortete mit Schreiben vom 28. September 2017, er könne der Forderung, jegliche Tätigkeiten im Bereich Kabel- und Funkaufklärung zu unterlassen, nicht entsprechen, da er das vom Parlament verabschiedete und vom Volk in einem Referendum angenommene Nachrichtendienstgesetz anwenden und vollziehen müsse und die Umsetzung dieses Gesetzes offensichtlich keine durch die Verfassung und die EMRK garantierten Grundrechte verletze. Darüber hinaus hätten die Gesuchstellenden kein schutzwürdiges Interesse im Sinn eines Sondernachteils gemäss Art. 25a VwVG (SR 172.021), weshalb die Voraussetzungen für den Erlass einer Verfügung über Realakte nicht gegeben seien. Dementsprechend trete der NDB auf die Anträge 1, 2, 4, 5 und 6 nicht ein. Antrag 3 werde als datenschutzrechtliches Einsichtsgesuch in die Datenbank des NDB entgegengenommen.

B. Mit Beschwerde vom 30. Oktober 2017 gelangten die Gesuchstellenden an das Bundesverwaltungsgericht. Sie beantragten in erster Linie, der NDB sei zu verpflichten, in einer Verfügung über ihre Anträge vom 31. August 2017 zu entscheiden oder die Sache zu materieller Behandlung an die zuständige Behörde weiterzuleiten. Der NDB teilte in der Beschwerdeantwort mit, seine Abklärungen hätten ergeben, dass keiner der Gesuchstellenden im Zusammenhang mit einem Funk- oder Kabelaufklärungsauftrag in der einschlägigen Datenbank verzeichnet sei. Die Funk- und Kabelaufklärung könne zwar mit Eingriffen in grundrechtlich geschützte Positionen einhergehen, die nötigen gesetzlichen Grundlagen dafür seien jedoch vorhanden und alle Anforderungen von Art. 36 BV und Art. 8 EMRK seien erfüllt.

BGE 147 I 280 S. 284

Mit Urteil vom 4. Juni 2019 wies das Bundesverwaltungsgericht die Beschwerde ab, soweit es darauf eintrat.

C. Dagegen haben die Gesuchstellenden am 8. Juli 2019 Beschwerde in öffentlich-rechtlichen Angelegenheiten an das Bundesgericht erhoben. (...) Das Bundesgericht heisst die Beschwerde gut und weist die Sache zu materieller Beurteilung der Gesuche an das Bundesverwaltungsgericht zurück. (Auszug)

Erwägungen

Aus den Erwägungen:

6. Eintretensvoraussetzung für Ansprüche nach Art. 25 Abs. 1 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) ist, dass ein Gesuch um Unterlassung, Folgenbeseitigung oder Feststellung eines widerrechtlichen Bearbeitens von Personendaten bei der zuständigen Behörde eingereicht wird. Die gesuchstellende Person muss partei- und prozessfähig sein und ein schutzwürdiges Interesse für ihr Begehren haben (WALDMANN/BICKEL, in: Datenschutzrecht, Grundlagen und öffentliches Recht, Belser/Epiney/ Waldmann [Hrsg.], 2011, S. 747 ff. §12 N. 156 und 160). Ob eine rechtswidrige Datenbearbeitung bereits erfolgt ist, noch andauert oder droht, d.h. in naher Zukunft ernstlich zu befürchten ist, ist grundsätzlich Teil der materiellen Prüfung (WALDMANN/BICKEL, a.a.O., S. 750 N. 161). Allerdings kann das Rechtsschutzinteresse fehlen, wenn bereits feststeht, dass die betreffenden Daten nicht oder nicht mehr bei der Behörde bearbeitet werden (JAN BANGERT, in: Basler Kommentar, Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, N. 32 zu Art. 25/25bis DSG; Urteil des BVGer A-6067/2008

vom 30. März 2009 E. 1.3.1).

6.1 Die Beschwerdeführenden haben mit Gesuch an den NDB (einer Bundesbehörde) die Widerrechtlichkeit der Funk- und Kabelaufklärung geltend gemacht und deren Unterlassung verlangt. Mit der Funk- und Kabelaufklärung werden Funksignale und grenzüberschreitende Datenströme erfasst und durchsucht. Die sich daraus ergebenden Informationen (insbesondere Kommunikationsinhalte und -randdaten) können in der Regel bestimmten Personen zugeordnet werden - wenn nicht im Zeitpunkt ihrer Erfassung, so doch nachträglich, eventuell unter Rückgriff auf zusätzliche Informationen oder technische Möglichkeiten (vgl. dazu BGE 136 II 508 E. 3.2 BGE 147 I 280 S. 285

S. 514 mit Hinweisen). Es handelt sich daher um Personendaten i.S.v. Art. 3 lit. a DSGVO. Jeder Umgang mit Personendaten stellt gemäss Art. 3 lit. e DSGVO ein Bearbeiten dar, unabhängig von den angewandten Mitteln und Verfahren. Dazu gehört insbesondere auch das Beschaffen von Daten (BGE 144 I 126 E. 4.1 S. 131). Vorliegend ist daher nicht erst das Weiterleiten von Daten an den NDB und die dort erfolgende Analyse und Speicherung von Daten relevant; bereits das elektronische Erfassen, Filtern und Durchsuchen von Daten durch das Zentrum für elektronische Operationen der Armee (nachfolgend: ZEO) stellt eine Datenbearbeitung dar (ISENRING/QUIBLIER, Der Preis der Sicherheit, in: Sicherheit & Recht 3/2017 S. 139; BERANEK ZANON/DE LA CRUZ BÖHRINGER, in: Datenschutzrecht: Beraten in Privatwirtschaft und öffentlicher Verwaltung, Handbücher für die Anwaltspraxis, Passadelis/Rosenthal/Thür [Hrsg.], 2015, S. 287 Ziff. 9.23). Davon ging grundsätzlich auch das Bundesverwaltungsgericht aus. Allerdings besteht vorliegend die Besonderheit, dass sich die Gesuche der Beschwerdeführenden nicht gegen konkrete, sie betreffende Massnahmen richten, sondern gegen das gesamte System der Funk- und Kabelaufklärung, wie es im Bundesgesetz vom 25. September 2015 über den Nachrichtendienst (NDG; SR 121) und den dazugehörigen Verordnungen vorgesehen ist. Ob dies zulässig ist oder - wie das Bundesverwaltungsgericht meint - auf eine unzulässige abstrakte Normenkontrolle hinausläuft, wird im Folgenden näher zu prüfen sein (vgl. unten E. 9).

6.2 Art. 25 Abs. 1 DSGVO setzt weiter das Bestehen eines schutzwürdigen Interesses voraus. Dieser Begriff findet sich auch in Art. 25 Abs. 2, Art. 25a und Art. 48 Abs. 1 lit. c VwVG sowie in Art. 89 Abs. 1 lit. c BGG.

6.2.1 Generell wird dafür vorausgesetzt, dass sich jemand in einer besonderen, nahen Beziehung zur Streitsache befindet und ihm das Verfahren einen unmittelbaren, praktischen Nutzen bringt. Zur Abgrenzung von der Popularbeschwerde und der Aufsichtsbeschwerde (Art. 71 VwVG) wird grundsätzlich verlangt, dass der Geschwister vom angefochtenen Akt besonders, d.h. stärker als jedermann, betroffen wird: Seine Betroffenheit muss sich von derjenigen der Allgemeinheit abheben (BGE 146 I 145 E. 4.1 mit Hinweisen). Sind viele Personen betroffen, ist massgebend, wie schwer die Einwirkungen auf den Einzelnen zu gewichten sind (BGE 144 II 233 E. 8.4 BGE 147 I 280 S. 286

S. 245 mit Hinweis). Wo die Grenze zur unzulässigen Popularbeschwerde verläuft, ist für jedes Rechtsgebiet gesondert zu beurteilen. Erforderlich ist eine praktisch vernünftige Abgrenzung, die sich am Rechtsschutzbedürfnis und an den weiteren Rechtsschutzmöglichkeiten orientiert (BGE 146 I 145 E. 4.1 mit Hinweisen). Ein schutzwürdiges Interesse ist insbesondere anzuerkennen, wenn dies erforderlich ist, um hinreichenden Grundrechtsschutz nach Art. 13 oder Art. 6 EMRK zu gewährleisten (vgl. z.B. BGE 144 I 126 E. 8.3.7 S. 153; BGE 128 I 167 E. 4.5 S. 174; BGE 123 II 402 E. 4b/aa S. 413; BGE 121 I 87 E. 1b S. 91 f.). Bei Ansprüchen nach Art. 25 Abs. 1 DSGVO wird ein schutzwürdiges Interesse grundsätzlich bejaht, wenn das Gesuch Daten betrifft, die sich direkt auf den Gesuchsteller beziehen oder Rückschlüsse auf ihn zulassen (WALDMANN/BICKEL, a.a.O., S. 749 § 12 N. 156 und 160; BANGERT, a.a.O., N. 33 f. zu Art. 25/25bis DSGVO).

6.2.2 Vorliegend ist streitig, inwiefern die Funk- und Kabelaufklärung Daten der Beschwerdeführenden betrifft. Der NDB hat im vorinstanzlichen Verfahren ausgeführt, dass die Beschwerdeführenden nicht im Zusammenhang mit einem Funk- oder Kabelauftrag in der einschlägigen Datenbank verzeichnet seien. Dies bedeutet aber nur, dass sie nicht Gegenstand eines konkreten Funk- oder Kabelaufklärungsauftrags waren: Wie der NDB selbst darlegt, enthält das Informationssystem Kommunikationsaufklärung (ISCO) nur die Daten zur Steuerung der Funk- und Kabelaufklärung (Art. 56 NDG; Art. 56 ff. der Verordnung vom 16. August 2017 über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes [VIS-NDB; SR 121.2]), insbesondere das Target (i.d.R. Telefonnummer), die Identitätsdaten der Zielperson sowie den Auftrag an das ZEO. Dass die Beschwerdeführenden in dieser Datenbank nicht verzeichnet sind, ist nicht verwunderlich, sind doch Angaben über schweizerische natürliche oder juristische Personen als Suchbegriffe unzulässig (Art. 39 Abs. 3 Satz 3 NDG). Dies schliesst jedoch nicht aus, dass Kommunikationen der Beschwerdeführenden im Rahmen von Funk- und Kabelaufklärungsaufträgen mit anderer Zielrichtung

erfasst, durchsucht und eventuell auch vom ZEO gespeichert oder an den NDB weitergeleitet wurden bzw. dies in naher Zukunft ernstlich zu befürchten ist. Bei der Funk- und Kabelaufklärung handelt sich um eine anlasslose Massenüberwachung von grenzüberschreitenden
BGE 147 I 280 S. 287

Telekommunikationsströmen. Wie die Beschwerdeführenden zutreffend darlegen, wird auch ein Grossteil der inländischen Kommunikation erfasst, der z.B. über Netzwerke und Server im Ausland erfolgt (ISENRING/QUIBLIER, a.a.O., S. 139; GERTSCH/STÄHLI, Nachrichtendienstlicher Staatsschutz, in: Schweizerisches Bundesverwaltungsrecht [SBVR], Bd. III/2, Sicherheits- und Ordnungsrecht des Bundes, Kiener/Bühler/ Schindler [Hrsg.], 2018, S. 429 Rz. 70). Zwar muss inländische Kommunikation ausgefiltert oder nachträglich gelöscht werden (Art. 39 Abs. 2 NDG); auch dies stellt jedoch eine Datenbearbeitung dar. Im Übrigen ist ungewiss, ob sämtliche inländische Kommunikation als solche erkannt und ausgesondert werden kann. Insofern sind die Beschwerdeführenden potenziell von der Funk- und Kabelaufklärung betroffen. Allerdings sind sie davon nicht speziell oder intensiver, sondern gleich betroffen wie alle anderen Kommunikationsteilnehmer und Internetnutzer auch. Fraglich ist, ob dies genügt, um ein schutzwürdiges Interesse an den gestellten Begehren zu begründen.

6.2.3 Speziell betroffen sind immerhin die Beschwerdeführenden 4-6 und 8 als Trägerinnen und Träger von Berufsgeheimnissen: Die Beschwerdeführenden 4-6 sind Medienschaffende und können sich auf den Schutz des Redaktionsgeheimnisses und den Quellenschutz nach Art. 10 EMRK und Art. 17 BV berufen (vgl. BGE 144 I 126 E. 4.1 S. 131 mit Hinweisen). Der Beschwerdeführer 8 unterliegt dem Anwaltsgeheimnis (Art. 13 des Bundesgesetzes vom 23. Juni 2000 über die Freizügigkeit der Anwältinnen und Anwälte [Anwaltsgesetz, BGFA; SR 935.61]). Die vertraulichen Kommunikationen zwischen Medienschaffenden und ihren Quellen bzw. zwischen Anwälten oder Anwältinnen und ihrer Klientenschaft geniessen besonderen Schutz: Gezielte Massnahmen zu ihrer Überwachung sind grundsätzlich ausgeschlossen (vgl. z.B. Art. 271 Abs. 1 StPO); besteht dennoch die Gefahr der Erfassung solcher Kommunikationen, sind besondere Vorkehrungen zu ihrem Schutz erforderlich (vgl. Art. 271 Abs. 3 StPO und Art. 16 lit. e des Bundesgesetzes vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF; SR 780.1]). Bei einer verdachtsunabhängigen Massenüberwachung besteht die Gefahr, dass auch solche besonders vertraulichen Kommunikationen erfasst, gescannt und ausgewertet werden, jedenfalls wenn keine besonderen Anordnungen, Verfahren und Kontrollen zu ihrem Schutz
BGE 147 I 280 S. 288

vorgesehen sind. Dies kann zu einem "chilling effect" führen, weil Journalisten und Anwälte nicht mehr auf die Vertraulichkeit ihrer elektronischen Kommunikationen mit Quellen bzw. Mandanten vertrauen (vgl. dazu Urteil des EGMR Big Brother Watch gegen Vereinigtes Königreich vom 13. September 2018 [Nrn. 58170/13, 62322/14 und 24960/15], § 492-495; so auch Urteil des deutschen Bundesverfassungsgerichts 1 vom 19. Mai 2020, BvR 2835/17 Rz. 193 ff.). Es besteht insofern ein besonderes, sich vom Interesse der Allgemeinheit abhebendes Schutzbedürfnis.

6.3 Die aufgeworfenen Fragen können offenbleiben, wenn alle Beschwerdeführenden (unabhängig vom Bestehen eines Berufsgeheimnisses) einen Anspruch auf materielle Behandlung ihrer Gesuche aus Art. 13 EMRK ableiten können. Dies ist im Folgenden zu prüfen, unter Berücksichtigung der Rechtsprechung des Bundesgerichts und des EGMR zum gebotenen Rechtsschutz gegen geheime Überwachungsmaßnahmen (unten E. 7-8) und der Gegenargumente des Bundesverwaltungsgerichts (unten E. 9).

7. Art. 13 EMRK gewährleistet mindestens, dass eine Person, die in vertretbarer Weise behauptet, Opfer einer Konventionsverletzung zu sein, bei einer nationalen Instanz eine wirksame Beschwerde einlegen kann. Dies muss nicht zwangsläufig ein Rechtsmittel an ein Gericht sein, sondern es genügt eine Beschwerdemöglichkeit an eine hinreichend unabhängige Verwaltungsbehörde. Die Wirksamkeit der Beschwerde beurteilt sich nach den Befugnissen der Behörde, den angefochtenen Akt gegebenenfalls aufzuheben bzw. dessen Auswirkungen beheben zu können; überdies müssen die notwendigen minimalen Verfahrensrechte gewährleistet sein, insbesondere der Anspruch auf rechtliches Gehör und auf die Begründung von Entscheidungen (vgl. zum Ganzen BGE 138 I 6 E. 6.1 S. 31 mit Hinweisen; Urteile des EGMR Leander gegen Schweden vom 26. März 1987, Serie A Bd. 116 § 77; Wille gegen Liechtenstein vom 28. Oktober 1999, Recueil CourEDH 1999-VII S. 331 § 75; je mit Hinweisen).

7.1 Im Zusammenhang mit geheimen Überwachungsmaßnahmen kann der Anspruch auf wirksamen Rechtsschutz eingeschränkt oder aufgeschoben werden, wenn und solange überwiegende Geheimhaltungsinteressen dies rechtfertigen und das Überwachungssystem insgesamt mit Art. 8 EMRK vereinbar ist (vgl. BGE 138 I 6 E. 6.2 S. 32 f. mit zahlreichen Hinweisen). Dazu ist jeweils

eine Gesamtschau vorzunehmen. Zu prüfen ist, ob das Gesetz angemessene BGE 147 I 280 S. 289

und wirksame Garantien gegen Missbrauch vorsieht, unter Berücksichtigung nicht nur der materiellen Garantien (Umfang, Dauer und Art der Überwachungsmaßnahmen, Voraussetzungen ihrer Anordnung, usw.), sondern auch der innerstaatlich zur Verfügung stehenden Kontroll- und Beschwerdemöglichkeiten und ihrer Effizienz (vgl. BGE 138 I 6 E. 6.2 S. 32 f.; Urteile Klass und Mitbeteiligte gegen Deutschland vom 6. September 1978, Serie A Bd. 28 § 50 ff.; Kennedy gegen Vereinigtes Königreich vom 18. Mai 2010, § 153 und 166 f.; Roman Zakharov gegen Russland vom 4. Dezember 2015, Recueil CourEDH 2015-III S. 309 § 232; Urteil Big Brother Watch, § 307 ff.). Insofern lassen sich die materiellen und formellen Anforderungen an geheime Überwachungssysteme nur schwer trennen; dies erschwert die Formulierung von allgemeingültigen Aussagen zum minimalen Rechtsschutz (BASIL CUPA, Rechtsschutz gegen präventive Überwachungsmaßnahmen am Beispiel des Nachrichtendienstes des Bundes, 2014, S. 67 Rz. 136). Dieser muss jedenfalls so wirksam wie möglich ausgestaltet werden (BGE 138 I 6 E. 6.2 S. 32; Urteil Leander, § 78 und 84).

7.2 Art. 13 EMRK ist vor dem Hintergrund der Subsidiarität der Individualbeschwerde an den EGMR zu sehen (Art. 35 Ziff. 1 EMRK). Jede Person, die nach Art. 34 EMRK befugt ist, Beschwerde wegen der Verletzung von Konventionsrechten an den EGMR zu führen, muss daher die Möglichkeit haben, ihre Ansprüche zuvor von einem innerstaatlichen Gericht oder mindestens einer unabhängigen innerstaatlichen Behörde überprüfen zu lassen (BGE 138 I 6 E. 1.3.2 S. 13 f.).

7.2.1 Zur Individualbeschwerde an den EGMR ist nach Art. 34 EMRK jede Person berechtigt, die in vertretbarer Weise behauptet, in einem durch die EMRK anerkannten Recht verletzt zu sein. Grundsätzlich wird verlangt, dass die Person direkt von einem Vollzugsakt betroffen ist, d.h. Art. 34 EMRK erlaubt i.d.R. nicht, sich gegen ein Gesetz in abstracto zu wenden, mit der Begründung, dass es die Konvention verletze (Urteil Klass, § 33 mit Hinweisen; Urteil Ouardiri gegen Schweiz vom 28. Juni 2011 [Nr. 65840/09], in: Plädoyer 2011 4 S. 66; AJP 2012 S. 557).

7.2.2 Ausnahmen von diesem Grundsatz werden jedoch insbesondere bei geheimen Überwachungsmaßnahmen zugelassen. Beschwerdeführenden soll damit die Möglichkeit eröffnet werden, an den Gerichtshof zu gelangen, wenn sie wegen des geheimen Charakters der angegriffenen Massnahmen keine konkrete, sie persönlich BGE 147 I 280 S. 290

berührende Massnahme angeben können. Nach Ansicht des Gerichtshofes müssen die Verfahrensvorschriften der Konvention in einer Art und Weise angewendet werden, die dazu dient, das System der Individualbeschwerde wirksam werden zu lassen ("effet utile"). Unter gewissen Voraussetzungen kann eine Person daher geltend machen, sie sei durch die blosse Existenz geheimer Massnahmen oder die solche Massnahmen gestattenden Gesetze Opfer einer Konventionsverletzung geworden (Urteil Klass, § 34). Im bereits erwähnten Grundsatzentscheid der Grossen Kammer Roman Zakharov (§ 171) differenzierte der EGMR die Anforderungen an die Beschwerdebefugnis, je nachdem, ob innerstaatlich wirksamer Rechtsschutz besteht. Ist dies nicht der Fall, so ist jedermann, der in den Anwendungsbereich des Gesetzes fällt, befugt, dagegen Beschwerde vor dem EGMR zu erheben, ohne auch nur behaupten zu müssen, konkret Opfer von Überwachungsmaßnahmen geworden zu sein. Besteht dagegen innerstaatlich wirksamer Rechtsschutz, müssen die Beschwerdeführenden darlegen, mit einer hinreichenden Wahrscheinlichkeit dem Risiko einer solchen Überwachung ausgesetzt zu sein ("probabilité raisonnable"; vgl. zu diesem Kriterium EGMR, Urteil Kennedy, § 122).

7.2.3 Im Urteil Big Brother Watch wandte der EGMR diese Grundsätze auf eine Beschwerde gegen das britische System der Massenüberwachung von Datenströmen sowie des Austauschs von Daten mit anderen Nachrichtendiensten an. Die Beschwerdebefugnis (Opferstellung) der beschwerdeführenden Personen und Organisationen wurde von der britischen Regierung weitgehend anerkannt und nur für den Datenaustausch zwischen Geheimdiensten bestritten (vgl. § 390). Der EGMR ging davon aus, dass im Vereinigten Königreich wirksamer Rechtsschutz durch das Investigatory Powers Tribunal (IPT) gewährleistet sei, einem unabhängigen Spezialgericht mit weitreichenden Untersuchungsbefugnissen, an das sich alle wenden können, die vermuten, Opfer einer geheimen Überwachungsmaßnahme zu sein, ohne dies nachweisen zu müssen (vgl. § 250 ff.). Der EGMR verlangte daher für die Beschwerdebefugnis die Glaubhaftmachung eines konkreten Risikos, dass Daten der Beschwerdeführenden vom Austausch zwischen den Geheimdiensten betroffen seien, was er bejahte (§ 393 f.).

8. Im Folgenden sind diese Grundsätze auf den vorliegenden Fall anzuwenden. BGE 147 I 280 S. 291

8.1 Die Beschwerdeführenden machen in vertretbarer Weise eine Verletzung ihrer durch die EMRK und - inhaltlich übereinstimmend - durch die Bundesverfassung geschützten Grundrechte geltend: Das Erfassen, Durchsuchen, Speichern und Weiterleiten von Daten stellt einen Eingriff in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung dar, die durch Art. 8 EMRK und Art. 13 BV geschützt sind. Sofern Kommunikationen von Medienschaffenden betroffen sind, ist auch Art. 10 EMRK und Art. 17 BV berührt. Für die Eintretensfrage kann daher offenbleiben, ob und inwiefern weitere Grundrechte von der Funk- und Kabelaufklärung berührt werden.

8.2 Da mit der Funk- und Kabelüberwachung breite Funk- und Datenströme erfasst werden, besteht das Risiko, dass auch Daten der Beschwerdeführenden bearbeitet werden (vgl. oben E. 6.2). Ob beim Durchsuchen dieser Daten "Hits" erzielt und Informationen an den NDB weitergeleitet und gespeichert werden, hängt von den verwendeten Suchbegriffen ab und kann nicht von vornherein ausgeschlossen werden. Auch wenn dies nicht der Fall sein sollte, d.h. die Daten vom ZEO nur zwischengespeichert oder sogar sofort gelöscht werden, stellt schon das Erfassen und Durchsuchen von Daten einen grundrechtsrelevanten Eingriff dar, der die für Art. 13 und 8 EMRK nötige minimale Intensität erreicht (entgegen der vom NDB vorinstanzlich vertretenen Auffassung): Es handelt sich um eine geheime Überwachung von vertraulichen Kommunikationen (Inhalte und Randdaten), die in der Regel dem Fernmeldegeheimnis unterliegen und z.T. durch Berufsgeheimnisse besonders geschützt sind. Im Entscheid Big Brother Watch (§ 338) verlangte der EGMR deshalb schon auf dieser Stufe Vorkehren zur Einschränkung des behördlichen Ermessens und zum Schutz vor Missbrauch. Im Übrigen lässt sich der Regelung in Art. 4 der Verordnung vom 17. Oktober 2012 über die elektronische Kriegsführung und die Funkaufklärung (VEKF; SR 510.292) und Art. 28 der Verordnung vom 16. August 2017 über den Nachrichtendienst (NDV; SR 121.1) entnehmen, dass gewisse Daten auch längerfristig beim ZEO gespeichert werden. Dies gilt insbesondere für Verbindungsdaten, die maximal 5 Jahre lang gespeichert und z.T. für weitere Aufträge verwendet werden dürfen (Art. 4 Abs. 4 VEKF; zur Randdatenspeicherung BGE 144 I 126 E. 4.2 S. 133 mit Hinweisen; Urteil Big Brother Watch, § 355-357; zit. Urteil des deutschen Bundesverfassungsgerichts, BvR 2835/17 Rz. 153 und 191).

BGE 147 I 280 S. 292

8.3 Nach dem Gesagten besteht eine hinreichende Wahrscheinlichkeit ("probabilité raisonnable"), dass Daten der Beschwerdeführenden von geheimen Massnahmen der Funk- und Kabelaufklärung betroffen werden, weshalb ihre "Opfereigenschaft" nach Art. 13 und 34 EMRK grundsätzlich zu bejahen ist.

9. Näher zu prüfen ist das Argument des Bundesverwaltungsgerichts, die Beschwerdeführenden hätten die Möglichkeit, über das datenschutzrechtliche Auskunftsrecht konkrete, sie betreffende Überwachungsmassnahmen anzufechten, und seien daher nicht darauf angewiesen, eine "abstrakte" Kontrolle der gesetzlichen Regelung der Funk- und Kabelaufklärung zu verlangen, was auf eine unzulässige abstrakte Normenkontrolle hinauslaufe.

9.1 Der Gesetzgeber hat eine abstrakte Normenkontrolle nur für kantonale Erlasse vorgesehen (Art. 82 lit. b und Art. 87 BGG), nicht aber für Bundeserlasse. Deren abstrakte Überprüfung kann grundsätzlich auch nicht auf dem Umweg über eine Feststellungsverfügung herbeigeführt werden (Urteil 1P.560/1999 vom 14. Februar 2000 E. 2c; KÖLZ/HÄNER/BERTSCHI, *Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes*, 3. Aufl. 2013, S. 122 Rz. 340). Personen, die sich durch bundesrechtlich vorgesehene Massnahmen in ihren Grundrechten verletzt fühlen, sind daher darauf angewiesen, konkrete, sie betreffende Vollzugsakte anzufechten. Zwar sind Bundesgesetze neben Völkerrecht für das Bundesgericht massgebend (Art. 190 BV), d.h. das Bundesgericht muss auch Gesetze, die sich nicht verfassungskonform auslegen lassen, anwenden und kann lediglich den Gesetzgeber einladen, die fragliche Bestimmung zu ändern (BGE 141 II 338 E. 3.1 S. 340; BGE 140 I 305 E. 5 S. 310; je mit Hinweis). Besteht allerdings ein echter Normkonflikt zwischen Bundes- und Völkerrecht, so geht grundsätzlich die völkerrechtliche Verpflichtung der Schweiz vor und eine dem Völkerrecht entgegenstehende Bundesgesetzgebung bleibt regelmässig unanwendbar. Dies gilt uneingeschränkt für Abkommen wie die EMRK, die Menschen- oder Grundrechte zum Gegenstand haben (grundlegend BGE 125 II 417 E. 4d S. 424 ff.; ständige Rechtsprechung vgl. BGE 144 I 126 E. 3 S. 130 mit Hinweisen; BGE 147 IV 182 E. 2.1). Insofern genügt die konkrete Kontrolle von Vollzugsakten grundsätzlich, um einen wirksamen Grundrechtsschutz sicherzustellen.

Davon geht, wie aufgezeigt (oben E. 7.2), auch die Rechtsprechung des EGMR aus, wonach in der Regel nur Vollzugsakte mit

BGE 147 I 280 S. 293

Individualbeschwerde angefochten werden können. Ein Abweichen von diesem Grundsatz ist nur gerechtfertigt, wenn es den Beschwerdeführenden nicht möglich oder nicht zumutbar ist, einen

Anwendungsakt abzuwarten oder zu verlangen und diesen innerstaatlich anzufechten (vgl. JULIEN MARQUIS, *La qualité pour agir devant la Cour européenne des droits de l'homme*, 2017, Rz. 1017, 1032 ff., 1041).

9.2 Das Bundesverwaltungsgericht verwies vorliegend auf die Möglichkeit, ein Auskunftsbegehren nach Art. 8 DSGVO zu stellen und im Anschluss daran Rechtsschutz gemäss Art. 25 i.V.m. 33 DSGVO zu erhalten. Es führte aus, den Beschwerdeführenden stünde mit dem datenschutzrechtlichen Auskunftsrecht die Möglichkeit offen, die Verletzung ihrer grund- und konventionsrechtlichen Ansprüche durch Massnahmen der Funk- und Kabelaufklärung zu rügen und eine rechtmässige Überwachung gerichtlich durchzusetzen. Es ging also davon aus, dass es den Beschwerdeführenden möglich sei, Auskunft über konkrete, sie betreffende Massnahmen der Funk- und Kabelaufklärung zu erhalten und diese anschliessend gerichtlich überprüfen zu lassen. Dies überzeugt nicht: Die mit der Funk- und Kabelaufklärung verbundenen Massnahmen sind geheim und werden den Betroffenen auch nachträglich nicht bekannt gegeben. Wie im Folgenden darzulegen sein wird, ermöglicht auch der datenschutzrechtliche Auskunftsanspruch keinen wirksamen Rechtsschutz gegen solche Massnahmen im Einzelfall.

9.2.1 Gemäss Art. 63 NDG wird die Auskunft aufgeschoben, wenn überwiegende Interessen an einer Geheimhaltung bestehen (Abs. 2), maximal bis zum Ende der Aufbewahrungsdauer der Daten (Abs. 4). Diese kann u.U. mehrere Jahrzehnte betragen (vgl. z.B. Art. 21 VIS-NDB zur Datenbank IASA NDB: Aufbewahrungsdauer bis zu 45 Jahre). Art. 36 Abs. 5 NDG sieht zwar vor, dass der NDB Daten aus Beschaffungen im Ausland, die mit genehmigungspflichtigen Beschaffungsmassnahmen vergleichbar sind, gesondert abspeichern kann, wenn der Umfang der Daten, die Geheimhaltung oder die Sicherheit dies erfordert; derartige Daten unterliegen einer maximalen Aufbewahrungsdauer von drei Jahren (Art. 70 Abs. 3 VIS-NDB). Es handelt sich jedoch um eine Kann-Vorschrift, deren Anwendungsbereich unklar ist.

9.2.2 Auch nach Wegfall des Geheimhaltungsinteresses kann mit einem Auskunftsersuchen an den NDB im Wesentlichen nur in
BGE 147 I 280 S. 294

Erfahrung gebracht werden, ob dieser Daten einer Person in seinen Informationssystemen speichert. Ob auch die Herkunft der gespeicherten Daten aus der Funk- und Kabelaufklärung mitgeteilt wird, ist ungewiss - dies wäre jedoch Voraussetzung für die Geltendmachung von Folgeansprüchen wegen widerrechtlicher Datenbearbeitung im Rahmen der Funk- und Kabelaufklärung. Gemäss Art. 8 Abs. 2 lit. a DSGVO schliesst die Auskunft "verfügbare Angaben" zur Herkunft der Daten ein. Dies würde voraussetzen, dass alle Informationen aus der Funk- und Kabelaufklärung bei der Überführung in die allgemeinen Informationssysteme des NDB als solche gekennzeichnet werden.

9.2.3 Jedenfalls aber stellen die in den Informationssystemen des NDB gespeicherten Daten nur einen Bruchteil der im Rahmen der Funk- und Kabelaufklärung erfassten, vom ZEO durchsuchten, gefilterten und sonstwie bearbeiteten Daten dar. Nach den Feststellungen des deutschen Bundesverfassungsgerichts zur Auslands-Telekommunikationsüberwachung in Deutschland werden täglich aus den zugänglich gemachten Datenströmen aufgrund eines mehrstufigen und vollautomatisierten Filterungs- und Auswertungsprozesses ca. 270'000 Telekommunikationsvorgänge sowie eine um mehrere Grössenordnungen höhere Menge von Verbindungsdaten selektioniert, gespeichert und anschliessend manuell auf ihre nachrichtendienstliche Relevanz überprüft, wobei durchschnittlich nur rund 260, d.h. 1 o/oo, als relevant identifiziert und weitergeleitet werden (zit. Urteil des deutschen Bundesverfassungsgerichts, BvR 2835/17 Rz. 24 f.). Es ist nicht auszuschliessen, dass die Grössenverhältnisse in der Schweiz vergleichbar sind. Ein Auskunftsersuchen an das ZEO (oder an den NDB über die beim ZEO gespeicherten Daten gemäss Art. 8 Abs. 4 DSGVO) würde nicht weiterhelfen, denn die dort bearbeiteten Daten sind (soweit überhaupt noch vorhanden) in der Regel noch nicht nach Personen aufgeschlüsselt und damit nicht auffindbar.

9.2.4 Das indirekte Auskunftsrecht nach Art. 64 f. NDG gewährleistet per se keine wirksame Beschwerdemöglichkeit nach Art. 13 EMRK, sondern stellt einen objektiven Kontrollmechanismus dar, welcher den Aufschub des Beschwerderechts teilweise kompensieren kann (BGE 138 I 6 E. 6.3 S. 33 und E. 7 S. 34 ff.). Es erscheint jedoch nicht gewährleistet, dass sich die Kontrolle des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und des

BGE 147 I 280 S. 295

Bundesverwaltungsgerichts auf die Datenbearbeitung im Rahmen der Funk- und Kabelaufklärung erstreckt; hierfür kann auf das zum datenschutzrechtlichen Auskunftsrecht Gesagte verwiesen werden.

9.3 Unter diesen Umständen ist es den Beschwerdeführenden nicht möglich, konkrete, sie betreffende Massnahmen der Funk- und Kabelaufklärung anzufechten. Sie sind deshalb darauf

angewiesen, das "System" der Funk- und Kabelaufklärung in der Schweiz überprüfen zu lassen. Dabei handelt es sich - entgegen der Auffassung des Bundesverwaltungsgerichts - nicht um eine abstrakte Normenkontrolle. Gegenstand der Prüfung ist nicht das Gesetz als solches, sondern die vermutete Erfassung von Daten der Beschwerdeführenden in der Funk- und Kabelaufklärung. Gefragt wird deshalb nicht, ob die Bestimmungen des NDG zur Funk- und Kabelaufklärung verfassungs- und konventionskonform gehandhabt werden könnten, sondern ob die (vermutete) Bearbeitung von Daten der Beschwerdeführenden im aktuellen System der Funk- und Kabelaufklärung deren Grundrechte verletzt. Dabei sind nicht nur die gesetzlichen Grundlagen, sondern auch allfällige interne Richtlinien und Weisungen, die effektive Vollzugspraxis von NDB und ZEO sowie die tatsächliche Kontrollpraxis der Aufsichtsbehörden zu berücksichtigen (vgl. oben E. 7.2.3).

9.4 Zwar sind gewisse Einschränkungen des Rechtsschutzes bei geheimen Überwachungsmaßnahmen zulässig; dies setzt jedoch voraus, dass das Gesamtsystem den Anforderungen von Art. 8 EMRK und Art. 13 BV genügt (vgl. oben E. 7.1). Dies muss auf entsprechende Rüge hin mindestens von einer unabhängigen Behörde überprüft werden können, bevor die betroffenen Personen mit Individualbeschwerde an den EGMR gelangen (oben E. 7.2). Im Urteil Big Brother Watch (§ 255 f.) betonte der EGMR die zentrale Bedeutung des innerstaatlichen Rechtsschutzes bei der Überprüfung von geheimen Massenüberwachungssystemen. Ohne die sorgfältige Prüfung von Funktionsweise und Umfang solcher Systeme durch die innerstaatlichen Gerichte, unter Berücksichtigung auch von vertraulichen Unterlagen zur Vollzugspraxis, sei es dem Gerichtshof unmöglich, die EMRK-Konformität solcher Regime zu kontrollieren. Es sei Aufgabe der nationalen Gerichte, die schwierige Abwägung der auf dem Spiel stehenden Interessen vorzunehmen, bevor diese vom EGMR überprüft würden. Dies setzt vorliegend

BGE 147 I 280 S. 296

voraus, dass auf die Gesuche der Beschwerdeführenden nach Art. 25 Abs. 1 DSG eingetreten wird. Dies entspricht dem Vorgehen im Fall BGE 144 I 126. Damals machten die Beschwerdeführer geltend, die Speicherung und Aufbewahrung ihrer Telekommunikationsranddaten widerspreche den Garantien der EMRK und der Bundesverfassung. Der Dienst Überwachung Post und Fernmeldeverkehr (ÜPF) trat auf die Feststellungs- und Unterlassungsbegehren der Beschwerdeführer ein, obwohl die streitige Verpflichtung in einem formellen Bundesgesetz verankert war (Art. 15 Abs. 3 des bis zum 28. Februar 2018 geltenden Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs [aBÜPF]) und die Beschwerdeführenden von der gesetzlich vorgesehenen Randdatenspeicherung nicht mehr, sondern gleich betroffen waren wie alle anderen Fernmeldeteilnehmerinnen und -teilnehmer in der Schweiz. Damit ermöglichte er eine unabhängige Überprüfung des Systems der Randdatenspeicherung durch das Bundesverwaltungsgericht.