Urteilskopf

144 I 126

13. Auszug aus dem Urteil der I. öffentlich-rechtlichen Abteilung i.S. A. und Mitb. gegen Dienst Überwachung Post- und Fernmeldeverkehr sowie X. AG und Y. AG (Beschwerde in öffentlich-rechtlichen Angelegenheiten) 1C_598/2016 vom 2. März 2018

Regeste (de):

Speicherung und Aufbewahrung von Randdaten der Telekommunikation.

Streitgegenstand bildet die verwaltungsrechtliche Frage, ob die Speicherung und Aufbewahrung von mit dem Fernmeldeverkehr verbundenen Randdaten konform mit der Verfassung bzw. der EMRK sind (E. 2.2). Art. 15 Abs. 3 des bis zum 28. Februar 2018 geltenden Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (aBÜPF) verpflichtete die Fernmeldedienstanbieter - gleich wie das heute geltende BÜPF -, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten ihrer Kunden zu speichern und während sechs Monaten aufzubewahren (E. 3). Die Speicherung und die Aufbewahrung von Randdaten stellen einen Eingriff in die Grundrechte der Betroffenen dar, insbesondere in das Recht auf Achtung des Privatlebens, das den Anspruch auf informationelle Selbstbestimmung miteinschliesst (E. 4). Die Intensität dieses Grundrechtseingriffs ist allerdings zu relativieren: Die gespeicherten Daten betreffen nicht den Inhalt der Kommunikation und werden von den Fernmeldeunternehmen weder gesichtet noch miteinander verknüpft; für einen Zugriff der Strafverfolgungsbehörden müssen die qualifizierten gesetzlichen Voraussetzungen der Strafprozessordnung erfüllt sein (E. 5). Art. 15 Abs. 3 aBÜPF bildete für die Randdatenspeicherung eine hinreichende gesetzliche Grundlage (E. 6). Die Randdatenspeicherung und -aufbewahrung dient namentlich der Aufklärung von Straftaten; damit liegt ein gewichtiges öffentliches Interesse vor (E. 7). Die datenschutzrechtlichen Bestimmungen sehen wirksame und angemessene Garantien zum Schutz vor Missbrauch und behördlicher Willkür vor. Unter diesen Rahmenbedingungen ist auch die sechsmonatige Aufbewahrungsdauer verhältnismässig (E. 8).

Regeste (fr):

Enregistrement et conservation de données secondaires de télécommunication.

L'objet du litige porte sur la question - de droit administratif - de savoir si l'enregistrement et la conservation de données secondaires de télécommunication sont conformes à la Constitution, respectivement à la CEDH (consid. 2.2). L'art. 15 al. 3 de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication, dans sa version en vigueur jusqu'au 28 février 2018 (aLSCPT), imposait aux fournisseurs de services de télécommunication - à l'instar de la loi actuellement en vigueur - l'enregistrement, et leur conservation durant six mois, des données permettant l'identification de leurs clients ainsi que les données relatives au trafic et à la facturation (consid. 3). L'enregistrement et la conservation de données secondaires de télécommunication portent atteinte aux droits fondamentaux des utilisateurs concernés, en particulier à leur droit au respect de la vie privée, qui comprend celui de l'autodétermination informationnelle (consid. 4). L'intensité de cette ingérence doit cependant être relativisée: les données conservées ne concernent pas le contenu des communications, elles ne sont pas visionnées par les entreprises de télécommunication ni mises en lien les unes avec les autres; l'accès des autorités pénales à ces informations est soumis aux conditions strictes du code de procédure pénale (consid. 5). L'art 15 al. 3 aLSCPT constituait une base légale suffisante pour la conservation des données secondaires (consid. 6). L'enregistrement et la conservation de telles données sont en particulier utilisés dans le cadre d'enquêtes pénales, ce qui relève d'un intérêt public important (consid. 7). Les dispositions en matière de protection des données prévoient des garanties efficaces et adéquates contre une utilisation abusive et l'arbitraire des autorités. Dans ces circonstances, une durée de conservation de six mois apparaît également proportionnée (consid. 8).

Regesto (it):

Memorizzazione e conservazione di dati marginali di telecomunicazione.

Oggetto del litigio è la questione di diritto amministrativo di sapere se la memorizzazione e la conservazione di dati marginali collegati con il traffico delle telecomunicazioni sono conformi alla Costituzione risp. alla CEDU (consid. 2.2). Secondo l'art. 15 cpv. 3, in vigore fino al 28 febbraio 2018, della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle comunicazioni (vLSCPT), gli offerenti di prestazioni di telecomunicazioni erano tenuti - come secondo la legge attualmente in vigore - a conservare per sei mesi i dati necessari all'identificazione degli utenti, come anche i dati relativi al traffico e alla fatturazione (consid. 3). La memorizzazione e la conservazione di dati marginali costituiscono un'ingerenza nei diritti fondamentali degli interessati, in particolare nel diritto al rispetto della vita privata, che comprende quello all'autodeterminazione informativa (consid. 4). L'intensità di questa ingerenza nei diritti fondamentali dev'essere tuttavia relativizzata: i dati memorizzati non concernono il contenuto della comunicazione e non vengono esaminati o correlati tra loro; l'accesso da parte delle autorità di perseguimento penale a queste informazioni presuppone l'adempimento delle qualificate condizioni legali del codice di diritto processuale penale (consid. 5). L'art. 15 cpv. 3 vLSCPT costituisce una base legale sufficiente per la memorizzazione di dati marginali (consid. 6). La memorizzazione e la conservazione di questi dati serve segnatamente - come la LSCPT attualmente in vigore - a chiarire reati penali; si è quindi in presenza di un interesse pubblico importante (consid. 7). Le norme sulla protezione di dati prevedono garanzie efficaci e adeguate per la tutela da abusi e dall'arbitrio delle autorità. In questi limiti anche la durata di conservazione di sei mesi è proporzionale (consid. 8).

Sachverhalt ab Seite 128

BGE 144 I 126 S. 128

A. A., B., C., D., E. und F. (nachfolgend: Gesuchsteller) wandten sich je mit Schreiben vom 20. Februar 2014 an den Dienst Überwachung Post- und Fernmeldeverkehr (nachfolgend: Dienst ÜPF) und stellten folgende identische Begehren: "1. [Die jeweilige Anbieterin von Fernmeldediensten] sei anzuweisen, die gemäss Art. 15 Abs. 3 BÜPF [Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1)] gespeicherten Verkehrs- und Rechnungsdaten des Gesuchstel lers zu löschen und deren Speicherung in Zukunft zu unterlassen, soweit die betroffenen Daten nicht für die Erbringung der vertraglichen Leistungen gegenüber dem Gesuchsteller zwingend erforderlich sind. 2. [Die jeweilige Anbieterin von Fernmeldediensten] sei anzuweisen bzw. zu verpflichten, keine gemäss Art. 15 Abs. 3 BÜPF gespeicherten Verkehrs- und Rechnungsdaten des Gesuchstellers an den Dienst ÜPF oder an andere Behörden oder an Gerichte herauszugeben. (...)"
B. Der Dienst ÜPF wies die jeweiligen Gesuche mit Verfügung vom 30. Juni 2014 ab, soweit er darauf eintrat. Die dagegen von den Gesuchstellern erhobenen Beschwerden wies das Bundesverwaltungsgericht mit Urteil A-4941/2014 vom 9. November 2016 ab, nachdem es die Verfahren vereinigt hatte.
C. Das Bundesgericht weist die Beschwerde der sechs Privatpersonen gegen diesen Entscheid ab. (Zusammenfassung)

Erwägungen

Aus den Erwägungen:

2. (...)

2.2 Streitgegenstand vor Bundesgericht bildet nach dem Gesagten einzig die Frage, ob die Speicherung und Aufbewahrung von mit dem Fernmeldeverkehr der Beschwerdeführer verbundenen Randdaten verfassungs- bzw. konventionskonform sind. Betroffen ist somit nur die verwaltungsrechtliche Seite des zweigeteilten Rechts der Überwachung des Post- und Fernmeldeverkehrs (vgl. dazu ausführlich E. 7.2 und E. 8.2 ff. des angefochtenen Entscheids). Vom Prozessthema nicht erfasst wird der Aspekt des Zugriffs auf diese Daten durch die Strafverfolgungsbehörden zu Überwachungszwecken, der in der Strafprozessordnung geregelt ist

(Art. 269 ff. StPO). Auf diesbezügliche Anträge, Rügen und Ausführungen der Beschwerdeführer
BGE 144 I 126 S. 129

in ihrer ohnehin weitschweifigen Eingabe kann von vornherein nicht eingetreten werden. Am Streitgegenstand vorbei zielen namentlich die Vorbringen, die Voraussetzungen für die Anordnung einer (rückwirkenden) Überwachung und die Überwachungstypen selbst seien nicht bzw. nicht genügend präzise im Gesetz formuliert und deren nachträgliche Genehmigung durch das Zwangsmassnahmengericht biete keinen hinreichenden Schutz, die Verwendung von Vorratsdaten zu Überwachungszwecken beschränke sich - insbesondere im Bereich von Internetdelikten - grundsätzlich nicht auf Fälle schwerer Kriminalität, gehe über das Notwendige hinaus und könne auch Drittpersonen betreffen, es bestehe keine hinreichende gesetzliche Grundlage für Kopfschaltungen und Antennensuchläufe (Rasterfahndung), zumal Letztere lediglich auf einer Verordnungsbestimmung basierten, es widerspreche dem Grundsatz, dass Zwangsmassnahmen einen hinreichenden Tatverdacht voraussetzten, wenn erst die Auswertung der gespeicherten Antennendaten einen solchen begründeten, der im Strafverfahren gewährleistete journalistische Quellenschutz sei unzureichend, durch die geheime Überwachung von Informanten eines Journalisten, über die Letzterer nicht orientiert werde, werde dessen Anspruch auf wirksame Beschwerde verletzt, die in der StPO vorgesehenen Verwertungsvebote böten keinen hinreichenden Schutz und der Nachrichtendienst könne auch ohne Vorliegen eines konkreten Tatverdachts auf Überwachungsdaten zugreifen.
3. Die Speicherung und Aufbewahrung von Randdaten der Telekommunikation ist in Art. 15 Abs. 3 aBÜPF (AS 2001 3096) geregelt. Danach sind die Anbieterinnen verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren. Die Beschwerdeführer stellen die Vereinbarkeit dieser Bestimmung mit der Bundesverfassung und der EMRK in Frage. Dabei ist zu berücksichtigen, dass Bundesgesetze neben Völkerrecht für das Bundesgericht massgebend sind (Art. 190 BV). Bundesgesetzen kann damit weder im Rahmen der abstrakten noch der konkreten Normenkontrolle die Anwendung versagt werden. Zwar handelt es sich dabei um ein Anwendungsgebot und kein Prüfungsverbot, und es kann sich rechtfertigen, vorfrageweise die Verfassungswidrigkeit eines Bundesgesetzes zu prüfen. Wird eine solche festgestellt, muss das Gesetz dennoch angewendet werden, und das Bundesgericht kann lediglich den Gesetzgeber einladen, die fragliche Bestimmung zu
BGE 144 I 126 S. 130

ändern (BGE 141 II 338 E. 3.1 S. 340; BGE 140 I 305 E. 5 S. 310, BGE 140 I 353 E. 4.1 S. 358 f.; BGE 139 I 180 E. 2.2 S. 185). 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 (BGE 142 II 35 E. 3.2 S. 39; BGE 139 I 16 E. 5.1 S. 28 f.; je mit Hinweisen). Dies gilt uneingeschränkt für Abkommen, die Menschen- oder Grundrechte zum Gegenstand haben, auf welche die sog. "Schubert"-Praxis (BGE 99 Ib 39 E. 3 und 4 S. 44 f.; vgl. ferner dazu BGE 142 II 35 E. 3.2 S. 39; BGE 136 III 168 E. 3.3.4 S. 172 f.) keine Anwendung findet.
4. Die Beschwerdeführer rügen, eine systematische und anlasslose Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs verletze das Recht auf Achtung des Intim-, Privat- und Familienlebens, den Schutz der Privatsphäre, einschliesslich die Achtung des Brief-, Post- und Fernmeldeverkehrs, den Schutz vor Missbrauch persönlicher Daten, die Meinungs- und Medienfreiheit, das Recht auf persönliche Freiheit, die Bewegungsfreiheit und die Unschuldsvermutung.
4.1 Art. 8 Ziff. 1 EMRK verankert namentlich den Anspruch jeder Person auf Achtung ihres Privat- und Familienlebens sowie ihrer Korrespondenz. Im Wesentlichen derselbe Schutz ergibt sich aus Art. 17 UNO-Pakt II (SR 0.103.2) und Art. 13 Abs. 1 BV (BGE 140 I 353 E. 8.3 S. 369; BGE 140 IV 181 E. 2.3 S. 183). Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) wird der Begriff des Privatlebens weit verstanden und ist keiner abschliessenden Definition zugänglich. Art. 8 Ziff. 1 EMRK umfasst insbesondere die Möglichkeit, Beziehungen zu anderen Menschen aufzubauen und zu entwickeln, und gewährleistet insoweit die Interaktion einer Person mit anderen (EGMR-Urteile Satakunnan Markkinapärssi Oy und Satamedia Oy gegen Finnland vom 27. Juni 2017 [Nr. 931/13] § 131; Magyar Helsinki Bizottság gegen Ungarn vom 8. November 2016 [Nr. 18030/11] § 191; Amann gegen Schweiz vom 16. Februar 2000 [Nr. 27798/95] § 65). Das Fernmeldegeheimnis, das die Privatsphäre schützt, trägt zur Verwirklichung dieser Garantien bei. Die Kommunikation mit fremden Mitteln wie Post und Telefon soll gegenüber Drittpersonen geheim erfolgen können. Immer wenn die Kommunikation durch eine Fernmeldedienstanbieterin erfolgt, soll sie unter Achtung der Geheimnissphäre vertraulich
BGE 144 I 126 S. 131

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; vielmehr werden auch die Randdaten des Kommunikationsvorgangs erfasst (BGE 140 I 353 E. 8.3 S. 369; BGE 140 IV 181 E. 2.3 f. S. 183 f.). Der Schutz der Privatsphäre umfasst den Anspruch jeder Person auf Schutz vor Missbräuchen ihrer persönlichen Daten (so ausdrücklich Art. 13 Abs. 2 BV). Im Bereich des Datenschutzes garantiert das verfassungsmässige Recht auf informationelle Selbstbestimmung, dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden (BGE 142 II 340 E. 4.2 S. 346; BGE 140 I 2 E. 9.1 S. 22 f.; BGE 138 II 346 E. 8.2 S. 359 f.). Der Begriff des Bearbeitens umfasst aus datenschutzrechtlicher Sicht auch das Beschaffen und Aufbewahren von Personendaten (Art. 3 lit. e des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz [DSG; SR 235.1]). Art. 10 EMRK und Art. 17 BV schützen die Medienfreiheit (BGE 141 I 211 E. 3.1 S. 213 f.). Die Verfassungsbestimmung gewährleistet ausdrücklich die Freiheit von Presse, Radio und Fernsehen sowie andere Formen der öffentlichen fernmeldetechnischen Verbreitung von Darbietungen und Informationen (Abs. 1). Die Zensur ist verboten (Abs. 2) und das Redaktionsgeheimnis garantiert (Abs. 3). Die Medienfreiheit 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 die Recherchetätigkeit der Journalisten zur Herstellung von Medienerzeugnissen und zu deren Verbreitung in der Öffentlichkeit (BGE 143 I 194 E. 3.1 S. 200). Als subsidiäres Auffanggrundrecht dazu gewährleistet die Meinungsfreiheit das Recht jeder Person, ihre Meinung frei zu bilden und sie ungehindert zu äussern und zu verbreiten (Art. 16 BV; BGE 137 I 209 E. 4.2 S. 211 f.). Der Schutzbereich umfasst die Gesamtheit der Mitteilungen menschlichen Denkens und alle möglichen Kommunikationsformen (BGE 127 I 145 E. 4b S. 151 f.). Die Meinungsfreiheit kann nicht nur durch direkte Eingriffe beeinträchtigt werden, sondern auch mittelbar, wenn der Einzelne aufgrund einer behördlichen

BGE 144 I 126 S. 132

Massnahme davon absieht, erneut von seinem Recht Gebrauch zu machen (sog. "chilling effect" oder "effet dissuasif"; BGE BGE 143 I 147 E. 3.3 S. 152 f.). Die Unschuldsvermutung gemäss Art. 6 Ziff. 2 EMRK und Art. 32 Abs. 1 BV gewährleistet, dass jede Person bis zur rechtskräftigen strafrechtlichen Verurteilung als unschuldig gilt. Sie verbrieft das Recht, als unschuldig behandelt zu werden, bis ein zuständiges Gericht nach Durchführung eines fairen Verfahrens die strafrechtliche Schuld in rechtsgenüglicher Weise nachgewiesen und festgestellt hat (Urteil 2C_1065/2014 vom 26. Mai 2016 E. 8.1, nicht publ. in: BGE 142 II 268). Im Allgemeinen gilt dabei das sog. Selbstbelastungsprivileg ("nemo tenetur se ipsum accusare"), das im Strafprozess ein Schweigerecht und ein Recht gewährleistet, nicht zu seiner eigenen Verurteilung beitragen zu müssen (BGE 142 IV 207 E. 8 S. 213 f.).

4.2 Die Speicherung und Aufbewahrung von Randdaten der Telekommunikation erfolgt unabhängig von einer allfälligen Strafuntersuchung und kann auch andere Zwecke verfolgen (z.B. die Suche und Rettung vermisster Personen; vgl. dazu E. 6.3 hernach). Daraus alleine lässt sich daher weder ein Verdacht noch eine Schuld im strafprozessualen Sinne ableiten (vgl. BGE 138 I 256 E. 4 S. 258). Inwiefern durch die Vorratsdatenspeicherung die Wahrscheinlichkeit steigen soll, als unschuldige Person eines Delikts verdächtigt zu werden, ist weder belegt noch leuchtet dies ein. Auch der EGMR anerkennt, dass die Aufbewahrung personenbezogener Daten nicht einem strafrechtlichen Vorwurf gleichgestellt werden kann (EGMR-Urteile S. und Marper gegen Grossbritannien vom 4. Dezember 2008 [Nr. 30562/04 und 30566/04] § 122; M.K. gegen Frankreich vom 18. April 2013 [Nr. 19522/09] § 36). Insofern vermag der Einwand, wonach der Staat alle Bürger als potenzielle Straftäter betrachte, nicht zu überzeugen. Ausserdem ist nicht ersichtlich, inwiefern mit der Erhebung von Randdaten ein gegen den "nemo tenetur"-Grundsatz verstossender Zwang ausgeübt werden soll: Soweit die Beschwerdeführer dieses Prinzip als verletzt erachten, weil die Datenspeicherung heimlich vorgenommen werde, ist ihnen entgegenzuhalten, dass die Beschaffung und Aufbewahrung von Randdaten der Telekommunikation klar aus Art. 15 Abs. 3 aBÜPF hervorgeht und somit nicht geheim erfolgt (vgl. JÜRGEN KÜHLING, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH
BGE 144 I 126 S. 133

zum Grundrechtsgericht, Neue Zeitschrift für Verwaltungsrecht 11/2014 S. 682). Demnach wird weder der "nemo tenetur"-Grundsatz noch die Unschuldsvermutung beeinträchtigt. Da die streitbetroffenen

Randdaten den Beschwerdeführern als Benutzer von Fernmeldediensten und Teilnehmer an Telekommunikationen grundsätzlich zugeordnet werden können, stellt deren Speicherung und Aufbewahrung indes einen Eingriff in ihr Recht auf informationelle Selbstbestimmung dar. Gleichermassen liegt nach der Rechtsprechung des EGMR durch die blosse Aufbewahrung von das Privatleben betreffenden Informationen, insbesondere wenn sie systematisch erfolgt (vgl. EGMR-Urteile Uzun gegen Deutschland vom 2. September 2010 [Nr. 35623/05] § 46; Rotaru gegen Rumänien vom 4. Mai 2000 [Nr. 28341/95] § 43 und 46), ein Eingriff in die von Art. 8 EMRK geschützten Rechte vor (EGMR-Urteile S. und Marper gegen Grossbritannien, § 67; Leander gegen Schweden vom 26. März 1987 [Nr. 9248/81] § 48; Gardel gegen Frankreich vom 17. Dezember 2009 [Nr. 16428/05] § 58; Brunet gegen Frankreich vom 18. September 2014 [Nr. 21010/10] § 31),unabhängig davon, ob die Daten zu einem späteren Zeitpunkt verwendet werden oder nicht (EGMR-Urteile Amann gegen Schweiz, § 69; Aycaguer gegen Frankreich vom 22. Juni 2017 [Nr. 8806/12] § 33).Überdies ist die mit der Speicherung und Aufbewahrung von Randdaten der Telekommunikation verbundene Informationsbeschaffung geeignet, in die insbesondere durch Art. 8 Ziff. 1 EMRK und Art. 13 Abs. 1 BV geschützte Privatsphäre derjenigen Personen einzugreifen, die auf solchen Wegen kommunizieren. Dem verfassungsmässigen Anspruch der persönlichen Freiheit (Art. 10 Abs. 2 BV) kommt hier keine darüber hinausgehende Bedeutung zu. Inwiefern die Bewegungs- und Versammlungsfreiheit tangiert sein sollen, legen die Beschwerdeführer nicht in rechtsgenüglicher Weise dar. Die Beschwerdeführer berufen sich im Weiteren auf die Meinungs- und Medienfreiheit. Ein direkter bzw. mittelbarer Eingriff erscheint insoweit nachvollziehbar, als durch die Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs eine Datenspur erfasst wird, die allenfalls Rückschlüsse auf das Kommunikationsverhalten der Betroffenen, auf die Recherchetätigkeit von Medienschaffenden sowie auf journalistische Quellen zulässt. Insoweit ist nicht auszuschliessen, dass Letztere davor zurückschrecken könnten, mit Journalisten in Kontakt zu treten. Ob diese Garantien tatsächlich

BGE 144 I 126 S. 134

tangiert sind, kann hier letztlich jedoch dahingestellt bleiben, da ohnehin die Voraussetzungen für die Einschränkung von Grundrechten zu prüfen sind.
5.

5.1 Gemäss Art. 8 Ziff. 2 EMRK darf in das Recht auf Achtung des Privatlebens nur eingegriffen werden, soweit dies 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. Nach der entsprechenden Bestimmung von Art. 36 BV bedürfen Einschränkungen von Grundrechten 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). Ein schwerer Eingriff in ein Grundrecht 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 143 I 194 E. 3.2 S. 201; BGE 141 I 211 E. 3.2 S. 214 f.).
5.2 Der EGMR geht bei der Möglichkeit einer detaillierten Profilbildung über intime Aspekte des Lebens davon aus, es liege ein besonders einschneidender Eingriff in das Privatleben ("particularly invasive interference [...] with private life") vor (EGMR-Urteil Szabó und Vissy gegen Ungarn vom 12. Januar 2016 [Nr. 37138/14]§ 70). Im gleichen Sinne schloss die Vorinstanz im vorliegenden Fall auf einen schweren Eingriff in das Recht der Beschwerdeführer auf Achtung ihres Fernmeldeverkehrs und ihres Anspruchs auf informationelle Selbstbestimmung. Sie begründete dies im Wesentlichen damit, bei den gespeicherten und aufbewahrten Randdaten der Telekommunikation handle es sich um einen sehr grossen Datensatz, der über das hinausgehe, was die Fernmeldedienstanbieterinnen für die Vertragserfüllung benötigten, und der ohne konkreten Anlass erstellt werde, insbesondere ohne dass ein Verdacht auf eine Straftat vorliege. Die erfassten Informationen könnten zu Persönlichkeitsprofilen über die Kommunikation der Beschwerdeführer verdichtet
BGE 144 I 126 S. 135

werden und liessen in ihrer Gesamtheit ohne Weiteres Rückschlüsse auf ihre persönlichen Lebensverhältnisse und ihr Umfeld zu, auch wenn es dabei "lediglich" um die äusseren Umstände der Kommunikation und nicht um deren Inhalt gehe. Überdies werde durch die Speicherung und

Aufbewahrung von Randdaten die Herrschaft der Beschwerdeführer über ihre personenbezogenen Daten beeinträchtigt. Deren mögliche Verwendung in einem späteren Strafverfahren wirke zusätzlich eingriffsbegründend bzw. -erschwerend, zumal ein "diffuses Gefühl des Überwacht- bzw. Beobachtet-Werdens" entstehen könne (sog. "chilling effect"; vgl. E. 9.4 des angefochtenen Entscheids).
Die Beschwerdeführer schliessen sich diesen Ausführungen im Wesentlichen an.
5.3 Diese Auffassung bedarf jedoch in mehrfacher Hinsicht einer differenzierten Beurteilung. Zunächst fällt relativierend ins Gewicht, dass es sich bei den gespeicherten und aufbewahrten Informationen lediglich um Randdaten und nicht um den Inhalt der Telekommunikation handelt. Dies wertet das Bundesgericht als deutlich weniger einschneidend als Fälle der inhaltlichen Kommunikationserfassung (BGE 142 IV 34 E. 4.3.2 S. 38 f.; BGE 139 IV 98 E. 4.2 S. 99). Auch der EGMR stuft die Eingriffsintensität je nach Art und Sensibilität der Daten unterschiedlich ein. So hielt er beispielsweise in Uzun gegen Deutschland dafür, dass die aus einer GPS-Überwachung gewonnenen Standortdaten - mithin Randdaten - von Informationen, die aus visuellen oder akustischen Überwachungen stammten, zu differenzieren seien, zumal Letztere empfindlichere Rückschlüsse auf das Verhalten, die Anschauungen und die Gefühle einer Person zuliessen und somit eher in das Recht auf Achtung des Privatlebens eingriffen (§ 52; ähnlich Urteil S. und Marper gegen Grossbritannien, § 86 und 120, wonach die Aufbewahrung von Fingerabdrücken aufgrund ihres geringeren Gehalts an sensiblen und persönlichen Informationen weniger schwere Auswirkungen auf das Privatleben habe als die Speicherung von Zellproben und DNA-Profilen).
5.4 Zwar trifft es zu, dass auch aus Randdaten in ihrer Gesamtheit gewisse Schlüsse auf das Privatleben der Benutzer von Fernmeldediensten gezogen werden können. So lassen sich daraus etwa Alltagsgewohnheiten, Aufenthaltsorte oder Ortswechsel sowie Informationen über berufliche und persönliche Kontakte, das Beziehungsnetz und das soziale Umfeld ableiten. Die Zusammenführung von
BGE 144 I 126 S. 136

Randdaten bzw. deren Kombination mit anderweitig erhobenen Daten ermöglicht somit, Profile zu erstellen, insbesondere Persönlichkeits- bzw. Bewegungsprofile oder solche über das Kommunikationsverhalten an sich. Aufgrund dessen liegt auch eine abschreckende Wirkung im Bereich der Nutzung von Fernmeldediensten nahe (vgl. Urteile Klass und andere gegen Deutschland vom 6. September 1978 [Nr. 5029/71] § 41; Szabó und Vissy gegen Ungarn, § 53). Die Möglichkeit der Verknüpfung von Randdaten, allenfalls in Kombination mit anderen Daten, besteht allerdings erst auf der Stufe der (rückwirkenden) Überwachung des Fernmeldeverkehrs, die einen zusätzlichen Eingriff bewirkt und vorliegend ausserhalb des Streitgegenstands liegt (vgl. E. 2.2 hiervor). Erst der Zugang zu den Randdaten und deren Auswertung im Einzelfall ermöglicht es den Strafverfolgungsbehörden, Erkenntnisse aus den gesammelten Informationen zu gewinnen und durch deren Verbindung allenfalls gewisse (Bewegungs-)Muster zu bilden. Demgegenüber werden die Randdaten auf der der Überwachung vorgelagerten Stufe der Speicherung und Aufbewahrung noch nicht zusammengeführt, weshalb auch keine sensiblen Profile gebildet werden können, die eine Beurteilung von wesentlichen Aspekten des Privatlebens erlauben würden. Ebenso wenig stehen die Randdaten den zuständigen staatlichen Stellen unmittelbar in ihrer Gesamtheit zur Verfügung. Vielmehr werden sie durch die einzelnen privaten Fernmeldedienstanbieterinnen erfasst und verbleiben während der Aufbewahrungsdauer in deren Sphäre, ohne dass eine Sichtung oder Verknüpfung mit anderen Daten stattfinden würde. Insofern ist zwischen zwei verschiedenen grund- und menschenrechtsrelevanten Massnahmen zu differenzieren, die eine unterschiedliche Eingriffsschwere aufweisen: Während die Speicherung und Aufbewahrung von Randdaten der Telekommunikation aufgrund der Masse der erfassten Daten und der grossen Anzahl der betroffenen Personen zwar wesentlich ist, nimmt der Eingriff mit dem Zugriff und der Nutzung dieser Daten durch die zuständigen Behörden erheblich an Intensität zu, wobei aber auch diesbezüglich anzumerken ist, dass die Anordnung einer rückwirkenden Überwachung im Einzelfall Verhältnismässigkeitsgesichtspunkten zu genügen hat, was allfälligen Profilbildungen enge Grenzen setzt.
5.5 Dass die Eingriffsintensität im Bereich von Art. 8 EMRK variieren kann, je nachdem ob die Erfassung von Randdaten der Telekommunikation oder deren Übermittlung an und Verwendung durch
BGE 144 I 126 S. 137

die zuständigen staatlichen Stellen betroffen ist, findet auch in der Rechtsprechung des EGMR ihre Stütze. Im Fall Malone gegen Grossbritannien war neben der Zulässigkeit einer inhaltlichen Telefonüberwachung zu beurteilen, ob die Weitergabe an die Polizei von Verbindungsranddaten, namentlich die gewählten Telefonnummern sowie der Zeitpunkt und die Dauer der Anrufe, die der Fernmeldedienstanbieter mittels eines speziellen Messsystems (sog. "metering" bzw. "comptage") aufgezeichnet hatte, konventionskonform ist. Der EGMR hielt dazu fest, die Erfassung solcher

Randdaten an sich, die von einer Uberwachung des Inhalts der Kommunikation unterschieden werden müsse, sei mit Blick auf die Konvention unbedenklich; erst die Übermittlung dieser Daten an die Polizei sei mit Blick auf Art. 8 EMRK problematisch (EGMR-Urteil vom 2. August 1984 [Nr. 8691/79] § 83 f.). Der Gerichtshof bestätigte diese Praxis in einem kürzlich ergangenen Entscheid, in dem die Konventionskonformität einer Aufzeichnung von Telekommunikationsranddaten (ein- und ausgehende Telefonate mit Teilnehmeridentifikation) und deren rückwirkende Überwachung zu überprüfen war (EGMR-Urteil Figueiredo Teixeira gegen Andorra vom 8. November 2016 [Nr. 72384/14] § 43). Diese Rechtsprechung legt in Übereinstimmung mit dem Vorerwähnten nahe, dass es sich bei der reinen Speicherung und Aufbewahrung von Randdaten der Telekommunikation nicht um einen schweren Eingriff handelt. Wie nachfolgend aufzuzeigen ist, läge indes selbst bei der Annahme eines solchen eine hinreichende gesetzliche Grundlage vor.
6.

6.1 Nach der Rechtsprechung des EGMR muss das Gesetz hinreichend präzise formuliert sein, damit die betroffenen Personen - nötigenfalls mit sachkundiger Hilfe - in einem nach den Umständen angemessenen Umfang die Folgen ihres Handelns vorhersehen können (EGMR-Urteile Kopp gegen Schweiz vom 25. März 1998 [Nr. 23224/94] § 64; Amann gegen Schweiz, § 56; S. und Marper gegen Grossbritannien, § 95; M.K. gegen Frankreich, § 27; Peruzzo und Martens gegen Deutschland vom 4. Juni 2013 [Nr. 7841/08 und 57900/12] § 35). Das Bundesgericht stellt gleichartige Anforderungen an die Regelungsdichte: Danach verlangt das Legalitätsprinzip gemäss Art. 36 Abs. 1 BV im Interesse der Rechtssicherheit und der rechtsgleichen Rechtsanwendung eine hinreichende und angemessene
BGE 144 I 126 S. 138

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 (BGE 143 I 310 E. 3.3.1 S. 314; BGE 139 I 280 E. 5.1 S. 284; je mit Hinweisen). Das Gebot der Bestimmtheit rechtlicher Normen darf dabei nicht absolut verstanden werden. Der Gesetzgeber kann nicht darauf verzichten, allgemeine und mehr oder minder vage Begriffe zu verwenden, deren Auslegung und Anwendung der Praxis überlassen werden muss (BGE 143 I 310 E. 3.3.1 S. 315; MEYER-LADEWIG/NETTESHEIM, in: EMRK, Handkommentar, Meyer-Ladewig und andere [Hrsg.], 4. Aufl. 2017, N. 105 zu Art. 8 EMRK). Der Grad der erforderlichen Bestimmtheit lässt sich nicht abstrakt festlegen. Er hängt unter anderem 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 143 I 253 E. 6.1 S. 264; BGE 141 I 201 E. 4.1 S. 204; BGE 139 I 280 E. 5.1 S. 284).
6.2 Soweit die Beschwerdeführer beanstanden, aus dem Gesetz gehe nicht klar hervor, welche Daten von den Fernmeldedienstanbieterinnen genau erfasst würden, kann ihnen nicht gefolgt werden. Denn an anderer Stelle in ihrer Rechtsschrift führen sie anhand einer exemplarischen Aufzählung aus, es würden systematisch Daten darüber gespeichert, wer mit wem, wann und von wo aus kommuniziere bzw. kommuniziert habe. Dies entspricht der vorinstanzlichen Umschreibung von Randdaten der Telekommunikation: Das Bundesverwaltungsgericht gelangte in überzeugender Auslegung der in Art. 15 Abs. 3 aBÜPF verwendeten unbestimmten Begriffe der "für die Teilnehmeridentifikation notwendigen Daten" sowie "Verkehrs- und Rechnungsdaten", auf die hier verwiesen wird (E. 10.6.2 f. des angefochtenen Entscheids; vgl. dazu ferner Art. 16 lit. d, Art. 24b und Ziff. 7 des Anhangs zur Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs [aVÜPF; AS 2001 3111]), zum Schluss, dass die Fernmeldedienstanbieterinnen verpflichtet seien, die mit dem Fernmeldeverkehr verbundenen äusseren Daten der Telekommunikation - im Gegensatz zu deren Inhalt - während sechs Monaten zu speichern und aufzubewahren. Die Beschwerdeführer selber lehnen sich mit ihrer Begriffserläuterung überdies zu Recht an die in Art. 8 lit. b nBÜPF vorgesehene
BGE 144 I 126 S. 139

Definition für Randdaten des Fernmeldeverkehrs an, die in materieller Hinsicht der geltenden Begriffsbestimmung entspricht (Botschaft vom 27. Februar 2013 zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [nachfolgend: Botschaft zum nBÜPF], BBl 2013 2683, 2739 Ziff. 2.6). Dabei handelt es sich um Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung (BBl 2016 1991). Insofern ist für jeden Benutzer von Fernmeldediensten bzw. jeden Teilnehmer an Telekommunikationen ersichtlich, dass die mit seinen Kommunikationsvorgängen zusammenhängenden äusseren Daten während sechs Monaten von den Anbieterinnen gespeichert und aufbewahrt werden, insbesondere auch ohne konkreten Verdacht auf

eine Straftat. Inwiefern es noch präziseren Angaben im Gesetz bedürfte, leuchtet nicht ein. Eine detaillierte Auflistung aller zu erfassenden Randdaten erwiese sich angesichts des zu ordnenden Sachverhalts und der damit einhergehenden Komplexität nicht als stufen- und sachgerecht (vgl. EGMR-Urteile Zakharov gegen Russland vom 4. Dezember 2015 [Nr. 47143/06] § 244 und 247; Malone gegen Grossbritannien, § 68; Kennedy gegen Grossbritannien vom 18. Mai 2010 [Nr. 26839/05] § 159; Szabó und Vissy gegen Ungarn, § 64). Eine solche Aufzählung wäre sehr technisch und für einen Laien - wie von den Beschwerdeführern selbst bemängelt - wohl kaum verständlich. Der Vorinstanz ist daher darin beizupflichten, dass es vorliegend für eine hinreichende gesetzliche Grundlage ausreichen muss, dass der Umfang und der Zweck der Speicherung und Aufbewahrung von Telekommunikationsranddaten in den Grundzügen im Gesetz festgelegt sind. Diesen Anforderungen genügt Art. 15 Abs. 3 aBÜPF, der eine Vorratshaltung von Randdaten für allfällige künftige Strafverfahren, zum Vollzug von Rechtshilfeersuchen, für die Suche und Rettung von vermissten Personen sowie für die nachrichtendienstliche Informationsbeschaffung bezweckt (vgl. Art. 1 Abs. 1 aBÜPF). Dass die Fernmeldedienstanbieterinnen dabei mehr Daten erfassen, als für die Rechnungsstellung notwendig ist, lässt sich aus dieser Bestimmung ermessen. Ausserdem ist für den Einzelnen aufgrund des Umfangs der Datenspeicherung voraussehbar, dass daraus - jedenfalls bei einer Verknüpfung mit weiteren Daten im Rahmen einer (rückwirkenden) Überwachung - sensible Informationen gewonnen werden können.
BGE 144 I 126 S. 140

6.3 Demnach bildet Art. 15 Abs. 3 aBÜPF eine hinreichende gesetzliche Grundlage für die Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs. Vor diesem Hintergrund durfte die Vorinstanz auch in willkürfreier, antizipierter Beweiswürdigung auf die Einholung der die Beschwerdeführer betreffenden Randdaten bei den jeweiligen Fernmeldedienstanbieterinnen verzichten, ohne dabei gegen den Anspruch auf rechtliches Gehör zu verstossen.
7. Wie bereits dargelegt, verfolgt die Vorratshaltung von Randdaten der Telekommunikation in erster Linie das Ziel, deren Verfügbarkeit mit Blick auf die Aufklärung und Verfolgung von Straftaten sicherzustellen. Mit der Vorinstanz ist daher davon auszugehen, dass die Speicherung und Aufbewahrung dieser Daten eine rückwirkende Überwachung als Mittel der Strafverfolgung ermöglicht. Diese Massnahmen dienen insofern nicht nur der im Gemeinwohl liegenden öffentlichen Sicherheit und Ordnung, indem sie zur Ermittlung und damit zur Verhütung von Straftaten beitragen (vgl. EGMR-Urteile S. und Marper gegen Grossbritannien, § 100; M.K. gegen Frankreich, § 29; Aycaguer gegen Frankreich, § 36; ferner Szabó und Vissy gegen Ungarn, § 55; Zakharov gegen Russland, § 232 und 237), sondern schützen ebenso die Rechte und Freiheiten Dritter (vgl. EGMR-Urteile Peruzzo und Martens gegen Deutschland, § 40; Uzun gegen Deutschland, § 77). Dies räumen denn auch die Beschwerdeführer im Grundsatz ein. Darüber hinaus bezweckt die Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs, die zuständigen Behörden bei der Suche und Rettung vermisster Personen zu unterstützen, womit ein Beitrag zur öffentlichen Gesundheit geleistet wird. Insofern liegt ein genügendes, sehr gewichtiges öffentliches Interesse vor.
8. Zu prüfen bleibt, ob die systematische Speicherung und Aufbewahrung von Randdaten der Telekommunikation verhältnismässig ist.
8.1 Die Beschwerdeführer stellen zunächst deren Eignung in Frage. Sie bemängeln, die Effektivität der Vorratsdatenspeicherung sei nicht empirisch erwiesen; vielmehr zeigten Studien auf, dass dieses Mittel weder einen Einfluss auf die Aufklärungsrate habe noch einen Abschreckungseffekt zeitige. Die Beschwerdeführer übersehen mit dieser Argumentation indes, dass es für einen Grundrechtseingriff unter dem Titel der Zwecktauglichkeit genügt, wenn er zur Erreichung des angestrebten Ziels geeignet ist, um vor dem Grundsatz

BGE 144 I 126 S. 141

der Verhältnismässigkeit standzuhalten (vgl. BGE 131 I 223 E. 4.3 S. 232; BGE 128 I 3 E. 3e/cc S. 15; je mit Hinweisen). Verlangt wird somit, dass die streitigen Massnahmen mit Blick auf den angestrebten Zweck Wirkungen zu entfalten vermögen und nicht gänzlich daran vorbei zielen (vgl. BGE 138 I 256 E. 6.2 f. S. 263 f.; BGE 137 IV 249 E. 4.5.2 S. 256 f.; BGE 135 II 105 E. 2.3.3 S. 109 f.; BGE 132 I 7 E. 4.2 S. 11 ff.). Dies ist bei der Speicherung und Aufbewahrung von Telekommunikationsranddaten ohne Weiteres der Fall, wie auch die von der Vorinstanz aufgeführten Beispiele aus der bundesgerichtlichen Rechtsprechung im Bereich der Strafverfolgung belegen (vgl. E. 12.5 des angefochtenen Entscheids). Durch die Vorratshaltung von Randdaten stehen den Strafverfolgungsbehörden zusätzliche Möglichkeiten zur Aufklärung von Straftaten zur Verfügung. Durch die weite Verbreitung und Nutzung von elektronischen Kommunikationsmitteln erweisen sich diese Massnahmen denn auch als nützliches Mittel für strafrechtliche Ermittlungen. Die Vorinstanz hat deren Eignung daher zu Recht bejaht. Überdies ist sie entgegen der Auffassung der

Beschwerdeführer nicht in Willkür verfallen, wenn sie den Verfahrensantrag, die Praxis zur Anordnung von rückwirkenden Überwachungen und deren richterliche Überprüfung seien zu evaluieren, in vorweggenommener Beweiswürdigung abgelehnt hat, soweit dieser denn überhaupt vom Streitgegenstand erfasst wird.
8.2 Die Beschwerdeführer bringen sodann vor, die systematische und anlasslose Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs seien nicht erforderlich, zumal die allermeisten der erfassten Daten nie in eine Strafuntersuchung einflössen. Diese Massnahmen müssten sich daher auf Angaben beschränken, die eng mit den untersuchten Delikten zusammenhingen. Im Vordergrund stünde dabei das sog. "quick freeze"-Verfahren, bei dem die Randdaten des Fernmeldeverkehrs erst bei aufkommendem dringendem Tatverdacht gesichert werden.

8.2.1 Soweit die Beschwerdeführer damit eine Eingrenzung der Vorratsdatenspeicherung in persönlicher, sachlicher und zeitlicher Hinsicht fordern, lehnen sie sich an die beiden Urteile des Gerichtshofs der Europäischen Union (EuGH) vom 8. April 2014 und 21. Dezember 2016 an. In ersterem Entscheid erklärte der EuGH die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten für ungültig, weil sich diese nicht auf das absolut Notwendige beschränke und somit unverhältnismässig sei. Dies begründete er unter anderem damit, dass sich die Richtlinie generell auf alle Personen, alle
BGE 144 I 126 S. 142

elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstrecke, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme vorzusehen. Insbesondere betreffe sie alle Personen, die elektronische Kommunikationsmittel benutzten, ohne dass diese auch nur mittelbar oder entfernt Anlass zur Strafverfolgung geben könnten. Auch verlange die Richtlinie keinen Zusammenhang zwischen den auf Vorrat gespeicherten Daten und der Bedrohung für die öffentliche Sicherheit. So beschränke sie sich weder auf Daten eines bestimmten Zeitraums, Gebiets oder eines Kreises von Personen, die in irgendeiner Weise in schwere Straftaten verwickelt sein oder aus anderen Gründen zur Verhütung oder Verfolgung solcher Delikte beitragen könnten. Zudem sehe die Richtlinie eine Mindestdauer von sechs Monaten für die Vorratsdatenspeicherung vor, ohne dass eine Unterscheidung der Datenkategorien je nach deren etwaigen Nutzen für das verfolgte Ziel oder anhand der betroffenen Personen getroffen werde (Urteil des EuGH vom 8. April 2014 C-293/12 und C-594/12 Digital Rights Ireland, Randnr. 57 ff.). Der EuGH bestätigte diese Rechtsprechung in seinem zweiten Urteil zur Vorratsdatenspeicherung, worin er zum Schluss gelangte, dass eine nationale Regelung, die eine allgemeine und unterschiedslose Speicherung von Daten vorsehe, aus den bereits genannten Gründen nicht vor Unionsrecht standhalte. Allerdings verbiete Letzteres den Mitgliedsstaaten nicht, eine Regelung zu erlassen, die eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermögliche, sofern sich diese hinsichtlich der Datenkategorien, der elektronischen Kommunikationsmittel, des Personenkreises und der Aufbewahrungsdauer auf das absolut Notwendige beschränke. Um diesen Erfordernissen zu genügen, müsse die nationale Regelung klar und präzise sein sowie ausreichende Garantien zum Schutz vor Missbrauchsrisiken enthalten. Sie habe anzugeben, unter welchen Umständen und Voraussetzungen eine Massnahme der Vorratsdatenspeicherung angeordnet werden dürfe. Insbesondere müsse sie auf objektive Anhaltspunkte gestützt sein, die es ermöglichten, diejenigen Personen zu erfassen, die einen zumindest mittelbaren Zusammenhang zu schweren Straftaten aufwiesen. Eine solche Begrenzung lasse sich auch durch ein geografisches Kriterium gewährleisten, wenn objektive Hinweise dafür bestünden, dass in gewissen Gebieten ein erhöhtes Risiko für die Vorbereitung oder Begehung von Straftaten bestehe (Urteil des EuGH vom 21. Dezember 2016 C-203/15 und C-698/15 Tele2 Sverige, Randnr. 108 ff.).
BGE 144 I 126 S. 143

8.2.2 Obschon diese Urteile für die Beurteilung der vorliegenden Streitsache nicht bedeutungslos sind, insbesondere weil sie die Rechtsfortbildung im europäischen Umfeld im Bereich der Vorratsdatenspeicherung entscheidend prägen und sich auch der EGMR in jüngeren Entscheiden darauf bezieht (vgl. EGMR-Urteile Szabó und Vissy gegen Ungarn, § 70; Zakharov gegen Russland, § 147), sind sie für die Schweiz nicht verbindlich (vgl. ASTRID EPINEY, Staatliche Überwachung versus Rechtsstaat: Wege aus dem Dilemma?, AJP 2016 S. 1507). Abgesehen von gewissen Zweifeln ob der Praktikabilität einzelner, darin vorgesehener Einschränkungen der Datenerfassung (vgl. dazu z.B. CHRISTOPH GRABENWARTER, Die Vorratsdatenspeicherung aus der Perspektive der EMRK, der Grundrechte-Charta und des Verfassungsrechts, in: Strafe und Prozess im freiheitlichen Rechtsstaat, Stuckenberg/Gärditz [Hrsg.], 2015, S. 786 f.), treffen sie die Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs auf Vorrat im Kern (vgl. HEINRICH WOLFF, Anmerkung zum Urteil des Europäischen Gerichtshofs vom 8.4.2014 zur

Vorratsdatenspeicherung, Die Offentliche Verwaltung 14/2014 S. 610; GRABENWARTER, a.a.O., S. 790; KÜHLING, a.a.O., S. 683; REINHARD PRIEBE, Reform der Vorratsdatenspeicherung - strenge Massstäbe des EuGH, Europäische Zeitschrift für Wirtschaftsrecht 12/2014 S. 457; ALEXANDER ROSSNAGEL, Die neue Vorratsdatenspeicherung, Neue Juristische Wochenschrift 8/2016 S. 539; BOEHM/ANDREES, Zur Vereinbarkeit der Vorratsdatenspeicherung mit europäischem Recht, Computer und Recht 3/2016 S. 153). Das Wesen der Vorratsdatenspeicherung besteht gerade darin, die von den Benutzern von Fernmeldediensten bei ihren Kommunikationsvorgängen generierten äusseren Daten über eine gewisse Zeitspanne zu erhalten, ohne zu wissen, ob sie für eine allfällige künftige Strafuntersuchung von Bedeutung sein werden oder nicht (vgl. WOLFF, a.a.O., S. 610; ANTONIE MOSER-KNIERIM, Vorratsdatenspeicherung, 2014, S. 139). Der schweizerische Bundesgesetzgeber hat sich ausdrücklich für dieses System der umfassenden und anlasslosen Speicherung und Aufbewahrung von Randdaten der Telekommunikation ausgesprochen und diesen Entscheid im Rahmen der Totalrevision des BÜPF bestätigt (vgl. Botschaft zum nBÜPF, BBl 2013 2683, 2740 f. Ziff. 2.6). Anlässlich der parlamentarischen Debatten im Nationalrat wurde die Einführung des von den Beschwerdeführern als mildere Massnahme vorgeschlagenen "quick freeze"-Verfahrens (zum Begriff vgl. E. 8.2 hiervor) explizit verworfen (Geschäft 13.025 zur
BGE 144 I 126 S. 144

Änderung des BÜPF, dritte Abstimmung zum Antrag der Minderheit IV, AB 2015 N 1165; vgl. ferner Voten Bundespräsidentin Simonetta Sommaruga, AB 2015 N 1160; NR Gabi Huber, AB 2015 N 1156; NR Jean Christophe Schwaab, AB 2015 N 1161; NR Beat Flach, AB 2015 N 1162). Dieses fällt als weniger weitreichende Massnahme ausser Betracht, zumal es eine geringere Zwecktauglichkeit aufweist als das geltende System und somit nicht den vom Gesetzgeber erwünschten Erfolg zu zeitigen vermag (vgl. BGE 129 I 35 E. 10.2 S. 46).
8.3 Das Gebot der Verhältnismässigkeit verlangt im Weiteren, dass ein vernünftiges Verhältnis zwischen den behördlichen Massnahmen, welche die angestrebten Ziele zu erreichen bezwecken, und den betroffenen öffentlichen oder privaten Interessen besteht (angemessene Zweck-Mittel-Relation; BGE 143 I 147 E. 3.1 S. 151, BGE 143 I 310 E. 3.4.1 S. 318; BGE 138 I 331 E. 7.4.3.1 S. 346; BGE 137 IV 249 E. 4.5 S. 256).
8.3.1 Der EGMR gesteht den Konventionsstaaten bei der vorzunehmenden Güterabwägung und damit bei der Beurteilung, ob eine Massnahme im Sinne von Art. 8 Ziff. 2 EMRK "in einer demokratischen Gesellschaft notwendig ist", einen gewissen Ermessensspielraum zu (EGMR-Urteile Leander gegen Schweden, § 59; Szabó und Vissy gegen Ungarn, § 57). Dabei anerkennt er, dass an der mit der Kriminalitätsbekämpfung bezweckten Wahrung der öffentlichen Sicherheit und Ordnung ein erhebliches Interesse besteht, weshalb sich eine Erfassung und Aufbewahrung von Informationen als notwendig erweisen kann (EGMR-Urteile Leander gegen Schweden, § 59; S. und Marper gegen Grossbritannien, § 105; Aycaguer gegen Frankreich, § 34). So sei es insbesondere aufgrund der heutigen Formen des modernen Terrorismus eine natürliche Folge, dass Regierungen auf neuste Technologien - einschliesslich massiver Kommunikationsüberwachungen - zurückgriffen, um solchen Anschlägen zuvorzukommen (EGMR-Urteile Szabó und Vissy gegen Ungarn, § 68; Klass und andere gegen Deutschland, § 48). Dennoch bedeute dies nicht, dass den Konventionsstaaten ein unbegrenztes Ermessen zustehe: Angesichts der Gefahr, dass die Demokratie mit der Begründung, sie zu verteidigen, durch (geheime) Überwachungen ausgehöhlt oder gar zerstört werde, dürften nicht jede beliebigen, als angemessen erachteten Massnahmen ergriffen werden (EGMR-Urteile Klass und andere gegen Deutschland, § 49; Leander gegen Schweden, § 60; Szabó und Vissy gegen Ungarn, § 57).
BGE 144 I 126 S. 145

In diesem Sinne hielt der EGMR dafür, dass die zeitlich unbeschränkte Aufbewahrung von Fingerabdrücken, Zellproben und DNA-Profilen in Datenbanken von bloss verdächtigen, nicht aber verurteilten Personen unverhältnismässig sei und somit nicht vor Art. 8 EMRK standhalte (EGMR-Urteile S. und Marper gegen Grossbritannien, § 125; M.K. gegen Frankreich, § 43; ferner ähnlich Brunet gegen Frankreich, § 44; vgl. e contrario EGMR-Urteile Peruzzo und Martens gegen Deutschland, § 49; Gardel gegen Frankreich, § 71 betreffend Datenbank für Sexualstraftäter). Ebenso erblickte er in der umfassenden und systematischen Überwachung aller Mobilfunkkommunikationen in Russland, auf die der Geheimdienst und die Polizei unmittelbar zugreifen konnten, eine Verletzung von Art. 8 EMRK (EGMR-Urteil Zakharov gegen Russland, § 302 ff.; vgl. ferner Mustafa Sezgin Tanrikulu gegen Türkei vom 18. Juli 2017 [Nr. 27473/06] § 65). Zum gleichen Ergebnis gelangte er im Entscheid Szabó und Vissy gegen Ungarn, in welchem ein geheimes Anti-Terror-Überwachungssystem zu beurteilen war, das nahezu alle Personen in Ungarn betraf und die massenhafte Überwachung von Kommunikationen erlaubte, ohne ausreichende und effektive Schutzmassnahmen vorzusehen, § 89). In diesem Urteil nahm der Gerichtshof ausserdem Bezug auf

den Entscheid Kennedy gegen Grossbritannien, in dem der Umstand, dass die dort zu beurteilende gesetzliche Grundlage keine unterschiedslose Überwachung von grossen Mengen von Kommunikationen erlaubte, ein wesentliches Element darstellte, um auf deren Konventionskonformität zu erkennen (§ 160; vgl. ähnlich Uzun gegen Deutschland, § 80).
8.3.2 Im vorliegenden Fall geht es zwar ebenfalls um die Beurteilung einer umfassenden und systematischen Datenerfassung. Allerdings ergeben sich ganz wesentliche Unterschiede zu den Sachverhalten, mit denen sich der EGMR in den vorgenannten Verfahren zu befassen hatte: Hinsichtlich der Art der gespeicherten Informationen geht es hier nicht um den Inhalt der Kommunikation, sondern bloss um deren äussere Umstände. Vor allem aber können die Strafverfolgungsbehörden auf die von den Fernmeldedienstanbieterinnen erfassten Daten nicht unmittelbar zugreifen und sie zu Untersuchungszwecken nutzen. Vielmehr kann ein solcher Zugriff erst auf der Stufe der Überwachung des Fernmeldeverkehrs erfolgen. Für deren Anordnung müssen die in der StPO vorgesehenen Voraussetzungen erfüllt sein, wobei es in verfahrensrechtlicher Hinsicht der
BGE 144 I 126 S. 146

Genehmigung durch ein unabhängiges Gericht bedarf. Darauf ist nachfolgend näher einzugehen. Neben der eigentlichen (inhaltlichen) Überwachung (Art. 270-272 i.V.m. Art. 269 StPO) sieht Art. 273 StPO die Möglichkeit vor, dass die Staatsanwaltschaft Auskünfte über die Verkehrs- und Rechnungsdaten bzw. die Teilnehmeridentifikation einholt. Voraussetzung für den Zugang zu solchen Randdaten des Fernmeldeverkehrs ist, dass der dringende Verdacht eines Verbrechens oder Vergehens (oder einer Übertretung nach Art. 179 septies StGB) besteht, dass die Schwere der Straftat die Überwachung rechtfertigt und dass die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden (Art. 273 Abs. 1 Ingress i.V.m. Art. 269 Abs. 1 lit. b und c StPO; BGE 141 IV 108 E. 4.4 S. 117 f.; BGE 137 IV 340 E. 5.2 S. 346 f.; EGMR-Urteile Uzun gegen Deutschland, § 70; Zakharov gegen Russland, § 243 ff.). Mithin haben die Auskünfte, die bis sechs Monate rückwirkend verlangt werden können (Art. 273 Abs. 3 StPO und Art. 15 Abs. 3 aBÜPF), dem Gebot der Verhältnismässigkeit zu genügen (Art. 197 Abs. 1 lit. c und d StPO; EGMR-Urteil Zakharov gegen Russland, § 260). Wie die inhaltliche Kommunikationsüberwachung (Art. 272 Abs. 1 StPO), bedürfen Massnahmen nach Art. 273 StPO der Genehmigung durch das Zwangsmassnahmengericht (Art. 273 Abs. 2 StPO), das gestützt auf die substanziierte und mit den wesentlichen Verfahrensakten belegte Eingabe der Staatsanwaltschaft (Art. 274 Abs. 1 StPO) innert fünf Tagen seit der Anordnung der Überwachung oder der Auskunftserteilung mit kurzer Begründung darüber entscheiden muss (Art 274 Abs. 2 StPO; EGMR-Urteile Klass und andere gegen Deutschland, § 55 f.; Szabó und Vissy gegen Ungarn, § 77). Dabei hat sich die Genehmigung namentlich darüber zu äussern, ob Vorkehren zum Schutz von Berufsgeheimnissen getroffen werden müssen (Art. 274 Abs. 4 lit. a StPO). Dokumente und Datenträger aus nicht genehmigten Überwachungen sind sofort zu vernichten und dürfen nicht verwendet werden (Art. 277 StPO; EGMR-Urteil Uzun gegen Deutschland vom 2. September 2010 [Nr. 35623/05] § 71 f.). Grundsätzlich teilt die Staatsanwaltschaft den überwachten Personen spätestens mit Abschluss des Vorverfahrens den Grund, die Art und die Dauer der Überwachung mit (Art. 279 Abs. 1 StPO; für Vorbehalte vgl. Art. 279 Abs. 2 StPO; EGMR-Urteile Klass und andere gegen Deutschland, § 58; Uzun gegen Deutschland, § 72; Szabó und Vissy gegen Ungarn, § 86).
BGE 144 I 126 S. 147

Ihnen steht dagegen der Beschwerdeweg offen (Art. 279 Abs. 3 StPO), der letztlich bis an das Bundesgericht führen kann (Art. 78 ff. BGG). Wird eine Überwachung des Fernmeldedienstes angeordnet, prüft der Dienst ÜPF unter anderem, ob die Überwachung eine gemäss dem anwendbaren Recht überwachungsfähige Straftat betrifft und von der zuständigen Behörde angeordnet worden ist (Art. 13 Abs. 1 lit. a aBÜPF). Er weist die Anbieterinnen an, die für die Überwachung notwendigen Massnahmen zu treffen (Art. 13 Abs. 1 lit. b aBÜPF) und nimmt die von ihnen übermittelten Randdaten entgegen, bevor er sie an die anordnende Behörde weiterleitet (Art. 13 lit. e aBÜPF und Art. 8 Abs. 3 aVÜPF; BGE 141 IV 108 E. 4.6 S. 118). Dabei setzt er die Vorkehren der Genehmigungsbehörde zum Schutz von Berufsgeheimnissen um und bewahrt die Überwachungsanordnung nach Einstellung der Massnahme während eines Jahres auf (Art. 13 Abs. 1 lit. f und i aBÜPF).
8.3.3 Aus diesen Ausführungen erhellt, dass die Strafverfolgungsbehörden keinen direkten und uneingeschränkten Zugriff auf die von den Fernmeldedienstanbieterinnen gespeicherten und aufbewahrten Randdaten der Telekommunikation haben. Vielmehr unterliegt dieser strengen Anforderungen, die insbesondere hinsichtlich des Personenkreises, der Art sowie des Umfangs der Daten zu massgeblichen Einschränkungen führen und zusammen mit zahlreichen Schutzmechanismen dazu beitragen, das Ermessen und die Zugriffsmöglichkeiten der Strafbehörden

einzudämmen. Die vorerwähnte Rechtsprechung des EGMR kann somit nicht unbesehen auf die vorliegende Streitsache übertragen werden.
8.3.4 Gleichwohl bedingt die Vorratshaltung von Randdaten des Fernmeldeverkehrs eine automatische Speicherung und Aufbewahrung einer grossen Menge von personenbezogenen Daten. Um insbesondere den Garantien von Art. 8 Ziff. 1 EMRK und Art. 13 BV zu genügen, verlangt der EGMR in Übereinstimmung mit dem Bundesgericht, dass diese systematische Datenerfassung und -aufbewahrung von angemessenen und wirkungsvollen rechtlichen Schutzvorkehrungen begleitet werden, so dass Missbräuchen und Willkür vorgebeugt werden kann (BGE 138 I 6 E. 4.3 S. 25; BGE 133 I 77 E. 5.4 S. 86 f.; vgl. BGE 136 I 87 E. 8.4 S. 116 f.; EGMR-Urteile Rotaru gegen Rumänien, § 59; S. und Marper gegen Grossbritannien, § 103; Kennedy gegen Grossbritannien, § 153; M.K. gegen Frankreich, § 32;

BGE 144 I 126 S. 148

Peruzzo und Martens gegen Deutschland, § 42; Zakharov gegen Russland, § 232; Szabó und Vissy gegen Ungarn, § 68).
8.3.5 Die Beschwerdeführer bemängeln in diesem Zusammenhang, die datenschutzrechtlichen Grundsätze würden nicht eingehalten und es bestehe kein hinreichender Schutz vor Missbrauch. Während das aBÜPF selbst keine Bestimmungen über den Datenschutz bzw. die Datensicherheit enthält, verweist Art. 9 Abs. 1 aVÜPF namentlich auf die Verordnung zum Bundesgesetz vom 14. Juni 1993 über den Datenschutz (VDSG; SR 235.11). In Art. 9 Abs. 2 aVÜPF wird überdies präzisierend festgehalten, dass die Fernmeldedienstanbieterinnen bei der Übertragung der Überwachungsdaten die Anweisungen des Dienstes ÜPF zu befolgen haben und sie für die Datensicherheit bis zum Übergabepunkt der Daten an den Dienst ÜPF verantwortlich sind. Die Richtlinien vom 22. Oktober 2015 über die organisatorischen und administrativen Anforderungen (OAR) sowie die technischen Anforderungen (TR TS) bei der rechtmässigen Überwachung des Fernmeldeverkehrs (vgl. Art. 33 Abs. 1bis aVÜPF; beide abrufbar unter www.li.admin.ch/de/dokumentation/downloads, besucht am 6. Dezember 2017) verweisen für die Gewährleistung der Datensicherheit durch die Fernmeldedienstanbieterinnen und den Dienst ÜPF auf das DSG (vgl. Ziff. 11.2 bzw. Ziff. 14.2), das ohnehin für Datenbearbeitungen durch private Personen oder Bundesorgane gilt (Art. 2 Abs. 1 DSG). Nach dessen Art. 7 müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden, wobei der Bundesrat nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit erlässt. Gemäss Art. 20 VDSG treffen die verantwortlichen Bundesorgane die nach den Art. 8-10 VDSG erforderlichen technischen und organisatorischen Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der Personen, über die Daten bearbeitet werden (Satz 1). Diese Bestimmung gilt nach den zutreffenden und unbestritten gebliebenen Ausführungen der Vorinstanz auch für die Fernmeldedienstanbieterinnen, zumal sie bei der Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs mit öffentlichen Aufgaben des Bundes betraut worden sind (Art. 3 lit. h DSG; vgl. E. 12.7.3 des angefochtenen Entscheids). Wer Personendaten bearbeitet bzw. ein Datenkommunikationsnetz betreibt, hat nach Art. 8 Abs. 1 VDSG für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu
BGE 144 I 126 S. 149

sorgen, um einen angemessenen Datenschutz zu gewährleisten. Die Systeme müssen dabei insbesondere gegen unbefugte oder zufällige Vernichtung (lit. a), zufälligen Verlust (lit. b), technische Fehler (lit. c), Fälschungen, Diebstahl oder widerrechtliche Verwendung (lit. d) sowie unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen (lit. e) geschützt werden. Geschuldet ist kein absoluter Schutz; vielmehr müssen die technischen und organisatorischen Massnahmen bei gesamthafter Beurteilung unter der Berücksichtigung des Zwecks, der Art und des Umfangs der Datenbearbeitung, der abschätzbaren Risiken für die betroffenen Personen und dem Stand der Technik angemessen sein (Art. 8 Abs. 2 VDSG; vgl. DAVID ROSENTHAL, Handkommentar zum Datenschutzgesetz, 2008, N. 3 f. zu Art. 7 DSG; BRUNO BAERISWYL, in: Datenschutzgesetz [DSG], 2015, N. 22 zu Art. 7 DSG). Solche Massnahmen sollen insbesondere bei automatisierten Datensammlungen und Informationssystemen verhindern, dass Daten unrechtmässig bearbeitet werden. Zu diesem Zweck definiert Art. 9 Abs. 1 VDSG verschiedene Zielsetzungen, die unter Beachtung des Verhältnismässigkeitsgebots umzusetzen sind. Dazu gehören namentlich Datenträger-, Transport-, Bekanntgabe-, Speicher-, Benutzer- und Zugriffskontrollen (zur Erläuterung dieser Begriffe vgl. Kommentar des Bundesamts für Justiz zur VDSG vom 14. Juni 2011, Ziff. 6.1.2; CHRISTA STAMM-PFISTER, in: Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl. 2014, N. 25 ff. zu Art. 7 DSG; ROSENTHAL, a.a.O., N. 19 zu Art. 7 DSG). Als technische oder organisatorische Schutzmassnahmen in Betracht

fallen beispielsweise Zugriffsbeschränkungen, Filter (wie z.B. Firewalls), Datenverschlüsselungen, sichere Systemkonfigurationen, Software zum Schutz vor Computerviren, -angriffen oder -spionage, Schulungen des Personals, Kontrollen und Protokollierungen (vgl. dazu auch Art. 10 VDSG; EGMR-Urteile Zakharov gegen Russland, § 272; Kennedy gegen Grossbritannien, § 165; ROSENTHAL, a.a.O., N. 8 f. zu Art. 7 DSG; BAERISWYL, a.a.O., N. 19 f. zu Art. 7 DSG).
8.3.6 Soweit die Beschwerdeführer beanstanden, es reiche für die Gewährleistung der Datensicherheit nicht aus, sich auf generell-abstrakte Bestimmungen zu berufen, vermögen sie nicht durchzudringen. Immerhin führen die vorerwähnten technischen, organisatorischen und administrativen Richtlinien des Dienstes ÜPF wichtige Massnahmen auf, die eine sichere Datenbearbeitung gewährleisten. So hat die Kommunikation von Informationen im Sinne einer Transport- und
BGE 144 I 126 S. 150

Bekanntgabekontrolle nur durch vorgängig authentifiziertes Personal und verschlüsselt zu erfolgen (OAR-Richtlinie, Ziff. 11.1 bzw. TR TS-Richtlinie, Ziff. 14.1). Zudem haben auf das System zur Abfrage von Informationen zu Fernmeldedienstabonnenten nur nutzungsberechtigte Personen mit User-Identifikation Zugang, die sich vorgängig beim Dienst ÜPF registrieren lassen müssen und von diesem einer Überprüfung unterzogen werden (Technische und Administrative Richtlinie vom 30. November 2004 für die Fernmeldedienstanbieterinnen zum Call Center Informationssystem, Ziff. 10, abrufbar unter www.li.admin.ch/de/dokumentation/downloads, besucht am 6. Dezember 2017). Damit wird den Zielsetzungen der Speicher-, Benutzer- und Zugriffskontrolle bei automatisierten Datensammlungen Nachachtung verschafft. Überdies müssen die Fernmeldedienstanbieterinnen genauso wie der Dienst ÜPF ihre Systeme vor unbefugtem Zugriff schützen und die involvierten Personen haben bei ihrer Tätigkeit die Vertraulichkeit der Informationen zu wahren (OAR-Richtlinie, Ziff. 11.3 f. bzw. TR TS-Richtlinie, Ziff. 14.3 f.). Ihnen drohen bei einem Verstoss gegen die berufliche Schweigepflicht (Art. 35 DSG) genauso wie bei einer Verletzung des Fernmeldegeheimnisses (Art. 43 des Fernmeldegesetzes vom 30. April 1997 [FMG; SR 784.10]) durch die Bekanntgabe gespeicherter Daten an Dritte (Art. 321ter StGB) strafrechtliche Sanktionen. Der damit einhergehende Abschreckungseffekt trägt insoweit zum Schutz vor missbräuchlichen Datenbearbeitungen bei (vgl. EGMR-Urteil Gardel gegen Frankreich, § 70), wenngleich ein rechtswidriges Verhalten von Einzelpersonen - wie der von den Beschwerdeführern kritisierte Verkauf oder das Verschwindenlassen von Daten - nie gänzlich ausgeschlossen werden kann (vgl. EGMR-Urteile Zakharov gegen Russland, § 270; Klass und andere gegen Deutschland, § 59). Abgesehen davon sind keinerlei Anzeichen dafür ersichtlich, dass Hacker oder ausländische Behörden auf Randdaten der Beschwerdeführer hätten zugreifen wollen bzw. schweizerische Fernmeldedienstanbieterinnen diese unbefugten Dritten zugänglich gemacht hätten. Die Beschwerdeführer sind denn auch weder in der Lage, ihre Befürchtungen zu belegen noch konkrete Hinweise namhaft zu machen.
Dass weder die Richtlinien des Dienstes ÜPF noch die Fernmeldedienstanbieterinnen vollständig und im Detail über die technischen und organisatorischen Massnahmen informieren, ist nicht zu beanstanden, zumal durch deren Offenlegung die damit verfolgten
BGE 144 I 126 S. 151

Sicherheitsziele massgeblich beeinträchtigt werden könnten (vgl. BAERISWYL, a.a.O., N. 33 zu Art. 7 DSG). Überdies vermag die Kontrolle durch den EDÖB, der seine Funktionen unabhängig und ohne Weisungen ausübt (Art. 26 Abs. 3 DSG), diesbezüglich Abhilfe zu verschaffen. Nach Art. 27 DSG überwacht er die Einhaltung der bundesrechtlichen Datenschutzvorschriften durch die Bundesorgane (Abs. 1), wobei er bei seinen Abklärungen Akten herausverlangen, Auskünfte einholen und sich die Datenbearbeitung vorführen lassen kann (Abs. 3 Satz 1). Insofern verfügt der EDÖB auch im Bereich der Speicherung und Aufbewahrung von Telekommunikationsranddaten durch die Fernmeldedienstanbieterinnen bzw. der Weiterleitung solcher Informationen an den Dienst ÜPF im Falle einer Überwachungsanordnung über umfassende Befugnisse zur Überprüfung der Datensicherheit. Dabei darf erwartet werden, dass er diesen Rechten im Rahmen seiner Aufsichtstätigkeit, die er von sich aus oder auf Ersuchen Dritter hin einleiten kann (vgl. RENÉ HUBER, in: Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl. 2014, N. 6 ff. zu Art. 27 DSG; YVONNE JÖHRI, in: Handkommentar zum Datenschutzgesetz, 2008, N. 6 zu Art. 27 DSG), auch tatsächlich nachlebt und insoweit Unregelmässigkeiten aufdeckt. Stellt er bei seinen Abklärungen eine Verletzung von Datenschutzbestimmungen fest, empfiehlt er dem verantwortlichen Bundesorgan, das Bearbeiten zu ändern oder zu unterlassen (Art. 27 Abs. 4 DSG). Gegen allfällige Verfügungen, die infolge abgelehnter oder nicht befolgter Empfehlungen ergehen können, kann er den Rechtsweg beschreiten (Art. 27 Abs. 5 und 6 DSG). Mangels gegenteiliger Anhaltspunkte oder Hinweise darf nach der Rechtsprechung des Bundesgerichts und des EGMR letztlich jedoch davon ausgegangen werden, dass die einschlägigen Datenschutzvorschriften zur sicheren Bearbeitung personenbezogener Informationen vorliegend eingehalten werden (vgl. BGE 137 I 167 E. 9.1.3 S. 191

f.; BGE 133 I 77 E. 5.4 S. 87; EGMR-Urteil Klass und andere gegen Deutschland, § 59). Dies gilt insbesondere auch mit Blick auf die (teilweise) Auslagerung der Datenbearbeitung ins Ausland. In Übereinstimmung mit den Ausführungen der Vorinstanz (vgl. E. 12.7.3 des angefochtenen Entscheids) muss sich der Auftraggeber insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG). Denn das Bundesorgan, das Personendaten durch Dritte bearbeiten lässt, bleibt für den Datenschutz verantwortlich (vgl. Art. 16 Abs. 1 DSG und Art. 22 Abs. 2 VDSG).
BGE 144 I 126 S. 152

Untersteht der Dritte dem DSG nicht, vergewissert es sich, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten, andernfalls stellt es diesen auf vertraglichem Weg sicher (Art. 22 Abs. 3 VDSG). Bei der Übertragung eines Teils der Datenbearbeitung an einen Dritten im Ausland - z.B. im Rahmen eines IT-Outsourcings - ist zudem Art. 6 DSG zu beachten (vgl. ROSENTHAL, a.a.O., N. 7 zu Art. 6 und N. 28 zu Art. 10a DSG; BÜHLER/RAMPINI, in: Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Auflage 2014, N. 6 zu Art. 10a DSG; EDÖB, Tätigkeitsbericht 18 [2010/2011], Datenübermittlung ins Ausland im Rahmen eines "Outsourcing"; a.M. BAERISWYL, a.a.O., N. 43 zu Art. 10a DSG). Nach dessen Abs. 1 dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Ein Indiz dafür, ob dies der Fall ist, lässt sich der Staatenliste des EDÖB entnehmen (Art. 31 Abs. 1 lit. d DSG i.V.m. Art. 7 VDSG; abrufbar unter www.edoeb.admin.ch/datenschutz/00626/00753/index.html, besucht am 6. Dezember 2017). Danach weist Rumänien, das von den Beschwerdeführern als Beispiel angeführt wird, entgegen ihrer Auffassung ein angemessenes Datenschutzniveau für das Bearbeiten von Daten natürlicher Personen auf. Insofern bieten die datenschutzrechtlichen Bestimmungen einen ausreichenden Schutz vor unbefugten Datenbearbeitungen und Zweckentfremdungen. Wie bereits an anderer Stelle ausgeführt (vgl. E. 7 hiervor), verfolgt die Vorratshaltung von Randdaten des Fernmeldeverkehrs primär das Ziel, deren Vorhandensein für allfällige künftige Strafverfahren zu gewährleisten (Art. 1 i.V.m. Art. 15 Abs. 3 BÜPF). Dies ist für die betroffenen Personen bereits bei der Datenbeschaffung erkennbar (vgl. E. 6.2 hiervor). Es leuchtet daher nicht ein, inwiefern ein Verstoss gegen den Bearbeitungsgrundsatz der Zweckbindung vorliegen soll.
8.3.7 Neben den vorgenannten Schutzmassnahmen stehen den Beschwerdeführern zusätzlich verfahrensrechtliche Garantien zum Schutz vor unsachgemässen Datenbearbeitungen zu. Im Vordergrund steht dabei das Auskunftsrecht nach Art. 8 DSG. Danach kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden (Abs. 1). Der Inhaber der Datensammlung muss der betroffenen Person alle über sie
BGE 144 I 126 S. 153

vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten (Abs. 2 lit. a) bzw. den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger mitteilen (Abs. 2 lit. b). Art. 9 DSG zählt allerdings verschiedene Gründe für eine Einschränkung des Auskunftsrechts auf. Nach dessen Abs. 1 lit. a kann der Inhaber einer Datensammlung die Auskunft verweigern, einschränken oder aufschieben, wenn ein Gesetz im formellen Sinn dies vorsieht.
Die Fernmeldedienstanbieterinnen berufen sich auf diese Ausnahme, um die Bekanntgabe der streitbetroffenen Randdaten an die Beschwerdeführer zu verweigern. Zur Begründung führen sie aus, das nur die Daten der Rechnungsstellung umfassende fernmelderechtliche Auskunftsrecht (Art. 45 FMG i.V.m. Art. 81 f. der Verordnung vom 9. März 2007 über Fernmeldedienste [FDV; SR 784.101.1]) gehe als lex specialis Art. 8 DSG vor. Dieser Argumentation kann indes nicht gefolgt werden. Die Fernmeldedienstanbieterinnen verkennen, dass der durch Art. 13 BV bzw. Art. 8 EMRK gewährleistete Anspruch auf Auskunft und Einsicht eine unentbehrliche Voraussetzung für die Verwirklichung des Schutzes der Privatsphäre darstellt (BGE 138 I 6 E. 7.5.2 S. 38 mit Hinweis). In diesem Sinne dient das Auskunftsrecht nach Art. 8 DSG der Durchsetzung des Persönlichkeitsschutzes, indem es den betroffenen Personen ermöglichen soll, die über sie in einer Datensammlung bearbeiteten Daten zu kontrollieren mit dem Ziel, die Einhaltung der datenschutzrechtlichen Grundsätze und Bestimmungen zu überprüfen und gegebenenfalls durchzusetzen (vgl. Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz, BBl 1988 II 413, 433 Ziff. 213.1; BGE 138 III 425 E. 5.3 S. 431 f.). Dies bezwecken denn auch die Beschwerdeführer mit ihren Auskunftsbegehren. Letztere erschöpfen sich nicht in der Verfolgung eines mit der Erbringung von Fernmeldedienstleistungen verbundenen Anspruchs im Sinne des FMG. Vielmehr zielen sie darauf ab, alle über sie in den Datensammlungen der Fernmeldedienstanbieterinnen vorhandenen Daten im Sinne des BÜPF in Erfahrung zu bringen, um

deren rechtmässige Bearbeitung zu überprüfen. Dass die in den Datensammlungen erfassten Randdaten der Telekommunikation über die blossen Daten zur Rechnungsstellung hinausgehen, räumen die Fernmeldedienstanbieterinnen denn auch selbst ein. Eingedenk der mit den Gesuchen der Beschwerdeführer verfolgten Zielsetzung bedeutete

BGE 144 I 126 S. 154

eine Beschränkung ihres Anspruchs auf das fernmelderechtliche Auskunftsrecht im Ergebnis, sie nicht nur der Möglichkeit zu berauben, die Einhaltung der materiellen Bestimmungen des Datenschutzes zu kontrollieren, sondern auch die Wahrnehmung ihrer übrigen Datenschutzrechte zu vereiteln (vgl. BGE 140 V 464 E. 4.2 S. 465; BGE 139 V 492 E. 3.2 S. 494; BGE 125 II 473 E. 4b S. 476). Dazu gehören namentlich die Ansprüche gemäss Art. 25 Abs. 1 DSG. Danach kann bei Vorliegen eines schutzwürdigen Interesses vom verantwortlichen Bundesorgan verlangt werden, dass es das widerrechtliche Bearbeiten von Personendaten unterlässt (lit. a), die Folgen eines widerrechtlichen Bearbeitens beseitigt (lit. b), oder die Widerrechtlichkeit des Bearbeitens feststellt (lit. c). Ferner verleiht Art. 25 Abs. 3 lit. a DSG dem Gesuchsteller namentlich das Recht auf Berichtigung unrichtiger Daten (vgl. dazu ferner Art. 5 Abs. 2 DSG). Gegen Verfügungen über solche datenschutzrechtlichen Ansprüche steht den betroffenen Personen der Rechtsweg offen (vgl. Art. 33 Abs. 1 DSG), womit sie die Sache einer Überprüfung durch ein unabhängiges Gericht zuführen können (vgl. JÖHRI, a.a.O., N. 39 zu Art. 25 DSG; MONIQUE STURNY, in: Datenschutzgesetz [DSG], 2015, N. 3 f. zu Art. 33 DSG). Im hier zu beurteilenden Fall stellen diese Rechte einen wirksamen Grundrechtsschutz sicher, zumal sie die Möglichkeit eröffnen, eine rechtmässige Speicherung und Aufbewahrung von Randdaten der Telekommunikation durch die Fernmeldedienstanbieterinnen gegebenenfalls auch gerichtlich durchzusetzen (vgl. EGMR-Urteil Zubkov und andere gegen Russland vom 7. November 2017 [Nr. 29431/05] § 129). Insofern geht es vorliegend nicht an, den Anspruch der Beschwerdeführer im Sinne einer Ausnahme nach Art. 9 Abs. 1 lit. a DSG auf die Daten der Rechnungsstellung zu verkürzen (vgl. dazu auch Erläuterungsbericht des Eidg. Departements für Umwelt, Verkehr, Energie und Kommunikation [UVEK] vom 15. Oktober 2014 zur Revision von Verordnungen zum FMG, S. 9, wonach Art. 81 Abs. 1 FDV wie bis anhin nicht beabsichtige, etwaige weitergehende, datenschutzrechtliche Auskunftsrechte einzuschränken). Vielmehr können sie sich auf das datenschutzrechtliche Auskunftsrecht gemäss Art. 8 DSG berufen, um alle Angaben in Erfahrung zu bringen, die sich auf ihre Person beziehen bzw. ihnen zugeordnet werden können (vgl. GRAMIGNA/MAURER-LAMBROU, in: Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl. 2014, N. 23 zu Art. 8 DSG). Soweit die Fernmeldedienstanbieterinnen in

BGE 144 I 126 S. 155

diesem Zusammenhang befürchten, die Gesuchsteller könnten durch das Auskunftsrecht sensible Informationen über andere Benutzer ihrer Fernmeldeanschlüsse erhältlich machen, vermag ihr Einwand nicht zu überzeugen. Denn wird ein Auskunftsbegehren einzig zum Zweck gestellt, eine andere Person auszuforschen, erweist es sich als rechtsmissbräuchlich (BGE 138 III 425 E. 5.5 S. 432; GRAMIGNA/MAURER-LAMBROU, a.a.O., N. 9 zu Art. 9 DSG). Ein solches Gebaren verdient von vornherein keinen Rechtsschutz, stellt es doch eine zweckwidrige Verwendung des Auskunftsrechts dar. Überdies ist mit dem EDÖB davon auszugehen, dass einer solchen Missbrauchsgefahr weitgehend mittels geeigneter, auf das jeweilige Kommunikationsmittel abgestimmter Authentifizierungsmassnahmen zur Eruierung des Benutzers eines Fernmeldeanschlusses begegnet werden kann. Inwiefern weitere Vorkehrungen zur Gewährleistung des Persönlichkeitsschutzes und des Fernmeldegeheimnisses von Drittpersonen ergriffen werden müssten, braucht hier nicht weiter geprüft zu werden.

8.3.8 Zur Durchsetzung einer rechtmässigen Datenbearbeitung durch die Bundesorgane steht den betroffenen Personen im Weiteren ein Anspruch auf Löschung bzw. Vernichtung zu (Art. 25 Abs. 3 lit. a DSG), der grundrechtlich geschützt ist (BGE 126 I 7 E. 3c/aa S. 12). Voraussetzung dafür ist, dass die Daten vom verantwortlichen Bundesorgan überhaupt nicht bzw. nicht mehr bearbeitet werden dürfen (vgl. JAN BANGERT, in: Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl. 2014, N. 58 zu Art. 25/25bis DSG; JÖHRI, a.a.O., N. 29 zu Art. 25 DSG; STURNY, a.a.O., N. 24 zu Art. 25 DSG). Dies ist insbesondere dann der Fall, wenn die Datenbearbeitung zur Erfüllung der öffentlichen Aufgabe nicht (mehr) erforderlich ist bzw. rechtmässig erhobene Daten zu lange aufbewahrt werden (vgl. BGE 120 Ia 147 E. 2a S. 150; EGMR-Urteil Zakharov gegen Russland, § 255; MÜLLER/SCHEFER, Grundrechte in der Schweiz, 4. Aufl. 2008, S. 169; KIENER/KÄLIN, Grundrechte, 2. Aufl. 2013, S. 180; SCHWEIZER/RECHSTEINER: in: Datenschutzrecht, 2015, Rn. 2.39). In seiner aktuellen Fassung sieht Art. 15 Abs. 3 BÜPF eine Aufbewahrungsdauer von sechs Monaten vor, weshalb die gespeicherten Randdaten der Telekommunikation nach deren Ablauf durch

die Fernmeldedienstanbieterinnen (unwiderruflich) zu löschen sind, sofern nicht spezielle Rechtfertigungsgründe eine längere Aufbewahrung gebieten (z.B. wenn das Entgelt für eine Fernmeldedienstleistung
BGE 144 I 126 S. 156

im Sinne von Art. 80 FDV weiterhin geschuldet ist). Die Löschungsverpflichtung nach sechs Monaten geht denn auch aus den Materialien zum aBÜPF hervor (Botschaft vom 1. Juli 1998 zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung, BBl 1998 IV 4241, 4268 Ziff. 212.22), weshalb davon auszugehen ist, dass die Telekommunikationsranddaten zur Erfüllung der damit verfolgten Zwecke, insbesondere die Vorratshaltung im Hinblick auf ein allfälliges künftiges Strafverfahren, jedenfalls nach geltendem Recht nicht mehr erforderlich ist. Soweit die Beschwerdeführer unter Hinweis auf BGE 139 IV 98 bezweifeln, dass die Telekommunikationsranddaten tatsächlich nach sechs Monaten gelöscht werden, kann ihnen nicht gefolgt werden. In diesem Urteil entschied das Bundesgericht zwar, dass bei Internetdelikten Art. 14 Abs. 4 aBÜPF, der keine zeitliche Befristung für die rückwirkende Datenerhebung enthält, als lex specialis dem Art. 273 Abs. 3 StPO vorgeht, der eine Auskunftserteilung bis sechs Monate rückwirkend vorsieht (vgl. E. 4.8 S. 101 f.). In BGE 139 IV 195 sprach es sich jedoch aus Gründen des Schutzes der Privatsphäre der Benutzer und Dritter, wie sie aus den Materialien zum neuen BÜPF hervorgehen, für die Einhaltung der Frist nach Art. 273 Abs. 3 StPO aus, der eine rückwirkende Überwachung für eine Dauer von höchstens sechs Monaten erlaubt (vgl. E. 2.3 S. 197 ff.). In diesem Sinne bestätigen die Fernmeldedienstanbieterinnen im vorliegenden Verfahren denn auch ausdrücklich, dass sie die gespeicherten Randdaten des Fernmeldeverkehrs nach sechs Monaten löschen.
8.3.9 Mit Blick auf die Aufbewahrungsdauer an sich bleibt anzumerken, dass die Aufklärung von Straftaten, welcher die Vorratshaltung von Randdaten der Telekommunikation in erster Linie dient, insbesondere im Bereich der Bekämpfung schwerer Delikte wie Terrorismus oder organisiertes Verbrechen, oft viel Zeit in Anspruch nimmt. Dabei handelt es sich ausserdem häufig um komplexe und umfangreiche Verfahren, in die viele Personen involviert sind (vgl. THOMAS HANSJAKOB, Die Vorratsdatenspeicherung in der Schweiz, Kriminalstatistik 1/2015 S. 56; ders., BÜPF/VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2. Aufl. 2006, N. 22 zu Art. 5 BÜPF). Vor diesem Hintergrund erweist sich der Aufbewahrungszeitraum von sechs Monaten, während dem die Strafverfolgungsbehörden die strengen Anforderungen für die Anordnung einer rückwirkenden
BGE 144 I 126 S. 157

Überwachung nachzuweisen haben (vgl. E. 8.3.2 f. hiervor), nicht als unverhältnismässig lange bemessen. Dies gilt umso mehr, als der EGMR im Entscheid Zakharov gegen Russland die im russischen Recht vorgesehene sechsmonatige Aufbewahrungsfrist für (inhaltliche) Überwachungsdaten der Mobilfunkkommunikation als vernünftig bezeichnete (§ 255).
8.4 Bei einer gesamthaften Betrachtung trifft es zwar zu, dass bei der Vorratshaltung von Randdaten der Telekommunikation sehr grosse Mengen an Daten erfasst werden und die Speicherung und Aufbewahrung alle Benutzer von Fernmeldediensten gleichermassen trifft, ohne dass diese Personen konkret Anlass zur Strafverfolgung geboten hätten. Auch ist nicht auszuschliessen, dass bereits das Wissen um die Datenerfassung und -aufbewahrung geeignet ist, das Kommunikationsverhalten zu beeinflussen. Die Beschwerdeführer berufen sich insoweit zu Recht auf ihre konventions- und verfassungsrechtlich geschützten Grundrechtspositionen. Diesen Schutzanliegen stehen jedoch gewichtige, im Gemeinwohl liegende Interessen am Schutz der öffentlichen Sicherheit und Ordnung sowie der öffentlichen Gesundheit entgegen, welche die Vorratshaltung der Telekommunikationsranddaten zu wahren bezweckten. Ausserdem ist die Eingriffsintensität insoweit zu relativieren, als es sich bei den gespeicherten und aufbewahrten Informationen lediglich um mit dem Fernmeldeverkehr verbundene, äussere Daten handelt, die nicht den Inhalt der Kommunikation betreffen. Entgegen der Auffassung der Beschwerdeführer werden die Randdaten überdies auf der Stufe der Speicherung und Aufbewahrung bei den einzelnen Fernmeldedienstanbieterinnen weder gesichtet noch miteinander verknüpft, weshalb auch keine sensiblen Profile erstellt werden können. Die Strafverfolgungsbehörden haben keinen unmittelbaren und uneingeschränkten Zugriff darauf. Vielmehr müssen die qualifizierten, in der StPO festgelegten Voraussetzungen erfüllt werden, damit eine rückwirkende Überwachung des Fernmeldeverkehrs vorgenommen werden kann.
Schliesslich sehen die datenschutzrechtlichen Bestimmungen zahlreiche wirksame und angemessene Garantien zum Schutz vor Missbrauch und behördlicher Willkür vor, denen ein automatisches System der Datenerfassung naturgemäss ausgesetzt ist. Insoweit können in der hier zu beurteilenden Speicherung und Aufbewahrung von Randdaten des Fernmeldeverkehrs keine Vorkehren erblickt werden, mit denen der demokratische Rechtsstaat mit der Begründung, ihn

zu verteidigen, untergraben oder gar zerstört würde. Unter Berücksichtigung, dass der EGMR den Konventionsstaaten im Rahmen von Art. 8 EMRK einen gewissen Ermessensspielraum zugesteht und er sich in seiner Rechtsprechung (noch) nicht einlässlich mit der Frage der Vorratshaltung von Randdaten der Telekommunikation befasst hat, erscheinen die Einschränkungen des Rechts auf Achtung des Privatlebens und des Anspruchs auf informationelle Selbstbestimmung nicht als unverhältnismässig. Kann mit anderen Worten nicht von vornherein auf die Konventionswidrigkeit des schweizerischen Systems der Vorratsdatenspeicherung geschlossen werden, überwiegen bei einer Gesamtwürdigung aufgrund des Vorerwähnten die öffentlichen Interessen an der Aufklärung von Straftaten bzw. an der Wahrung der öffentlichen Gesundheit die privaten Interessen der Beschwerdeführer an der Löschung resp. Unterlassung einer künftigen Speicherung ihrer Telekommunikationsranddaten. Die Rüge der Verletzung von Grundrechten, insbesondere Art. 8 EMRK und Art. 13 BV, erweist sich somit als unbegründet. Die von den Beschwerdeführern angeführten Urteile ausländischer Verfassungsgerichte sowie die weiteren von ihnen beigebrachten Dokumente und Stellungnahmen vermögen an dieser Beurteilung nichts zu ändern. Da der Eingriff insoweit gerechtfertigt ist, bedarf es entgegen ihrer Auffassung überdies keiner Einwilligung in die Speicherung und Aufbewahrung der Randdaten ihres Fernmeldeverkehrs.