Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

Abteilung I
A-4941/2014

Urteil vom 9. November 2016

Besetzung

Richterin Christine Ackermann (Vorsitz),
Richterin Claudia Pasqualetto Péquignot, Richterin Marianne Ryter, Richter Jürg Steiger, Richter Maurizio Greppi,
Gerichtsschreiber Benjamin Kohle.

Parteien

1. **A.**_____,
2. **B.**_____,
3. **C.**_____,
4. **D.**_____,
5. **E.**_____,
6. **F.**_____,

alle vertreten durch lic. iur. Viktor Györffy, Rechtsanwalt,
Peyrot, Schlegel und Györffy Rechtsanwälte,
Beethovenstrasse 47, 8002 Zürich,
Beschwerdeführer,

gegen

Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF),
Fellerstrasse 15, 3003 Bern,
Vorinstanz,

Gegenstand

Vorratsspeicherung von Randdaten der Fernmeldekommunikation.

Sachverhalt:

A.
A._____, B._____, C._____, D._____, E._____ und F._____ (nachfolgend: Gesuchsteller) gelangten mit Schreiben je vom 20. Februar 2014 an den Dienst Überwachung Post- und Fernmeldeverkehr (nachfolgend: Dienst). Sie stellten dem Dienst übereinstimmend folgende Anträge:

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 Gesuchstellers 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;

   unter Kosten- und Entschädigungsfolge zu Lasten des Staates.

Die Gesuchsteller äusserten sich vorab zur (sachlichen) Zuständigkeit des Dienstes. Sie gingen (sinngemäss) davon aus, das Speichern von Daten zur Teilnehmeridentifikation sowie von Verkehrs- und Rechnungsdaten (nachfolgend: Randdaten; vgl. zur Begrifflichkeit auch nachfolgend E. 4.2.2) durch die privaten Anbieterinnen von Fernmeldedienstleistungen (nachfolgend: Anbieterinnen) sei als Realakt zu qualifizieren, der in schwerwiegender Weise ihre Grundrechte einschränke. Aus diesem Grund hätten sie ein schutzwürdiges Interesse daran, dass der Dienst als die für die Überwachung des Fernmeldeverkehrs zuständige (Aufsichts-)Behörde die Anbieterinnen anweise, gespeicherte Randdaten zu löschen, die Speicherung in Zukunft zu unterlassen und keine gespeicherten Randdaten an den Dienst, an Behörden und an Gerichte herauszugeben.

In der Sache wandten sich die Gesuchsteller gegen die Speicherung der Randdaten ihres gesamten Fernmeldeverkehrs und deren sechsmonatige Aufbewahrung. Die Speicherung und Aufbewahrung der Randdaten tangiere ihre grund- und völkerrechtlich geschützte Privatsphäre, insbesondere die Achtung des Fernmeldeverkehrs und den Schutz vor Missbrauch

persönlicher Daten. Zudem sahen die Gesuchsteller ihre persönliche Freiheit, ihre Meinungs-, Medien- und Versammlungsfreiheit sowie die Garantie der Unschuldsvermutung eingeschränkt bzw. verletzt. Die Speicherung der Randdaten sei eine schwerwiegende Einschränkung ihrer Grundrechte, umso mehr, als sie sich nicht auf Daten beschränke, welche für die Erbringung der vertraglichen Leistungen notwendig seien. Hierfür fehle es bereits an einer hinreichend bestimmten formell-gesetzlichen Grundlage. Das BÜPF enthalte lediglich unbestimmte Rechtsbegriffe; nach Art. 15 Abs. 3 BÜPF seien die Anbieterinnen verpflichtet, "die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten" während sechs Monaten aufzubewahren. Dies sei zu wenig bestimmt, als dass Betroffene ermessen könnten, welche Randdaten zu welchem Zweck konkret gespeichert und aufbewahrt würden. Entsprechendes ergebe sich auch aus den anwendbaren Verordnungsbestimmungen nicht in hinreichender Weise. Vielmehr müsse auf die Richtlinien des Dienstes zurückgegriffen werden, die in ihren (technischen) Details allerdings nur für Spezialisten verständlich seien. Nach Ansicht der Gesuchsteller werden von den Anbieterinnen (gestützt auf die Richtlinien des Dienstes) insbesondere folgende Randdaten gespeichert:

– Grunddaten des Kunden, wie Name, Adresse, Geburtsdatum, Ausweis(nummer), Beruf, Telefonnummer sowie E-Mail-Adresse

– bei der Nutzung von Telefondienstleistungen die beteiligten Telefonnummern samt der Anbieter, die Vertragsdaten wie die Art des Vertrages, Angaben zum Inhaber des Anschlusses einschliesslich der Adresse(n), Angaben zu Zahlungen für den Anschluss wie die Art der Zahlung, Bankdaten und Kontonummer, Angaben zum Anruf wie Uhrzeit, Dauer, Art der Verbindung, Kosten sowie allfällige Um- oder Weiterleitungen

– bei Anrufen über ein Mobilfunknetz zusätzlich die International Mobile Subscriber Identity (IMSI), die International Mobile Equipment Identity (IMEI), die Personal Unblocking Keys (PUK1 und PUK2) sowie Beginn und Ende der Verbindung zu den genutzten Antennen

– beim Versand von SMS oder MMS zusätzlich Angaben zu Art, Status und Übertragung der Nachricht sowie die E-Mail-Adresse bei der Übertragung via einen Gateway

– beim Versand einer E-Mail die E-Mail-Adressen, Angaben zum Konto wie Inhaber (einschliesslich Adresse) und Bezahlung (einschliesslich Kontonummer), Angaben zur Übertragung des E-Mails wie Uhrzeit, Übertragungsprotokoll, Übertragungsart und Übertragungsstatus, Internet-Protocol-Adressen (IP-Adressen) der kommunizierenden Stellen, die Message-ID sowie Angaben zur Aufnahme der Verbindung zum E-Mail-Server

– bei der Nutzung des Internets Angaben zum Provider, Angaben zum Abonnement wie Inhaber (einschliesslich Adresse) und Bezahlung (einschliesslich Kontonummer), IP-Adressen, die Media Access Control Adresse (MAC-Adresse), den Ort der Einwahl und weitere Angaben zum Modem bzw. Router sowie beim Zugang auf das Internet über ein Mobilfunknetz Angaben über die benutzten Antennen bzw. deren Standort und Hauptstrahlrichtung.

Vor diesem Hintergrund und angesichts des Umfangs der Randdaten, welche gespeichert und aufbewahrt würden, sei die Bestimmung von Art. 15 Abs. 3 BÜPF auch insofern zu wenig präzise formuliert, als dass Betroffene ihr Verhalten danach richten bzw. die Folgen ihres Verhaltens voraussehen könnten. Ebenso wenig sei ein (überwiegendes) öffentliches Interesse ersichtlich, welches die Einschränkung ihrer Grundrechte rechtfertige. Zwar werde angeführt, die Überwachung des Fernmeldeverkehrs und damit auch die Speicherung der Randdaten diene der Verhinderung von Straftaten und der Beweissicherung. Die Effektivität der Speicherung von Randdaten wie etwa der Einfluss auf die Aufklärungsrate oder eine abschreckende Wirkung durch ein höheres Nachweisrisiko lasse sich jedoch nicht belegen.

Schliesslich sahen die Gesuchsteller die anlasslose Speicherung der Randdaten im Widerspruch zum Verhältnismässigkeitsgrundsatz sowie zu weiteren (allgemeinen) Rechtsgrundsätzen etwa im Bereich des Datenschutzes stehen. Ihrer Ansicht nach ist die anlasslose Speicherung von Randdaten nicht erforderlich, sondern – angesichts der Schwere des Grundrechtseingriffs – in zeitlicher und personeller Hinsicht zu beschränken, etwa indem Randdaten erst bei aufkommendem dringendem Tatverdacht gesichert würden (sog. quick freeze). Zudem sei weder die Datensicherheit gewährleistet noch würden die Anbieterinnen verpflichtet, die Randdaten nach sechs Monaten zu löschen. Ferner bemängeln D._____ sowie E._____, die beide als Journalisten tätig sind, die strafprozessualen Bestimmungen betreffend die Erhebung von Randdaten

durch die (Strafverfolgungs-)Behörden, da sie das Berufsgeheimnis wie etwa den Quellenschutz von Journalisten nicht in hinreichendem Mass wahren würden.

B.

Der Dienst wies die Gesuche mit Verfügungen je vom 30. Juni 2014 ab, soweit beantragt worden war, es seien die Anbieterinnen anzuweisen, gespeicherte Randdaten zu löschen und die Speicherung in Zukunft zu unterlassen (Antrag Ziff. 1). Soweit die Gesuchsteller beantragt hatten, es seien die Anbieterinnen anzuweisen, keine Randdaten an den Dienst oder an eine andere Behörde oder an Gerichte herauszugeben (Antrag Ziff. 2), trat er auf die Gesuche nicht ein. Schliesslich auferlegte es den Gesuchstellern Verfahrenskosten in der Höhe von je Fr. 500.–.

Der Dienst hielt zunächst in formeller Hinsicht fest, er sei als die für die Fernmeldeüberwachung zuständige Behörde zum Erlass der vorliegenden Verfügungen sachlich zuständig. Er bejahte zudem im Allgemeinen ein schutzwürdiges Interesse der Gesuchsteller am Erlass der anbegehrten Verfügungen. Soweit diese jedoch verlangten, es seien die Anbieterinnen anzuweisen, keine Randdaten herauszugeben (Antrag Ziff. 2), fehle es ihnen an einem aktuellen schutzwürdigen Interesse, weshalb insofern nicht auf die Gesuche einzutreten sei; der Rechtsschutz im Zusammenhang mit konkreten Überwachungsmassnahmen richte sich nach den Bestimmungen der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0).

In der Sache betrachtete der Dienst den Eingriff in den grund- und völkerrechtlich geschützten Anspruch auf Achtung des Fernmeldeverkehrs (nachfolgend: Fernmeldegeheimnis) bzw. das Recht auf Achtung des Privatlebens als schwer. Er erwog, dass zwar die Verpflichtung der Anbieterinnen, die Randdaten des Fernmeldeverkehrs zu speichern, nicht direkt dazu führe, dass der Staat Zugriff darauf erhalte. Die Speicherung der Randdaten sei jedoch genau auf diesen Zweck hin zugeschnitten und die umfangreiche Menge an Randdaten mit hoher Aussagekraft erlaube einen tiefen Einblick in das Privatleben Betroffener. Entgegen der Ansicht der Gesuchsteller bestehe hierfür – insbesondere angesichts der technischen Komplexität der Materie – eine hinreichende formell-gesetzliche Grundlage. Der Gesetzgeber habe in den Grundzügen festgelegt, welche Daten zu speichern und unter welchen Voraussetzungen diese an die (Strafverfolgungs-)Behörden herauszugeben seien. Der Umfang der zu speichernden Randdaten werde auf Verordnungsstufe in einer für interessierte Laien

verständlichen Sprache und schliesslich in den Richtlinien des Dienstes weiter konkretisiert. Die Speicherung der Randdaten liege sodann im öffentlichen Interesse an einer wirksamen Strafverfolgung und sei geeignet, Straftaten zu verhindern sowie Beweise zu sichern. Nach den Erwägungen des Dienstes ist der Eingriff in das grundrechtlich geschützte Fernmeldegeheimnis zudem erforderlich, da mit der Speicherung von Randdaten des Fernmeldeverkehrs eine rückwirkende Überwachung und damit eine Ermittlungsmöglichkeit eröffnet werde, die ohne sie nicht bestehen würde. Und schliesslich sei der Eingriff – insbesondere mit Blick auf die strafprozessualen Bestimmungen im Zusammenhang mit der Erhebung von Randdaten – auch zumutbar; für die Erhebung von Randdaten gelte der Grundsatz der Subsidiarität und die Erhebung bedürfe der Genehmigung durch das Zwangsmassnahmengericht. Diese Vorkehren rechtfertigten auch den mit der Speicherung verbundenen (mittelbaren) Eingriff in die Meinungsfreiheit.

Nach den abschliessenden Erwägungen des Dienstes trifft es zwar zu, dass der Gesetzgeber den Anbieterinnen im Zusammenhang mit der Speicherung von Randdaten keine konkreten Vorgaben betreffend den Datenschutz mache. Die Anbieterinnen seien jedoch gestützt auf die (allgemeinen) datenschutzrechtlichen Bestimmungen und damit technologieneutral verpflichtet, die Vertraulichkeit und Integrität der Daten zu gewährleisten. Damit werde den Anforderungen des Datenschutzes hinreichend Rechnung getragen.

C.

Gegen die Verfügungen des Dienstes (nachfolgend: Vorinstanz) vom 30. Juni 2014 liessen die Gesuchsteller (nachfolgend: Beschwerdeführer) je mit Schreiben vom 2. September 2014 Beschwerde beim Bundesverwaltungsgericht führen (Verfahren A-4941/2014, A-4946/2014, A-4948/2014, A-4950/2014, A-4954/2014 und A-4955/2014). Sie beantragen übereinstimmend, es seien die Verfügungen der Vorinstanz vom 30. Juni 2014 aufzuheben und es sei die jeweilige Anbieterin anzuweisen, gespeicherte Randdaten zu löschen und deren Speicherung zu unterlassen, soweit die Daten nicht für die Erbringung der vertraglichen Leistungen erforderlich seien (Antrag Ziff. 1). Zudem sei die jeweilige Anbieterin anzuweisen, dem Dienst oder einer anderen Behörde keine Randdaten herauszugeben (Antrag Ziff. 2).

Die Beschwerdeführer verweisen zunächst auf die gesetzlichen Bestimmungen und die (gerichtliche) Praxis im Zusammenhang mit der Speicherung und Erhebung von Randdaten und führen (erneut) aus, welche Randdaten gestützt darauf offenbar gespeichert würden. Sie sind der Ansicht, dass die anlasslose Speicherung von Randdaten der gesamten Telekommunikation in schwerwiegender Weise insbesondere in das grundrechtlich geschützte Fernmeldegeheimnis und die Meinungsfreiheit eingreife, zumal sie einen Grossteil der Bevölkerung betreffe und sich nicht auf Daten beschränke, welche für die Erbringung der vertraglichen Leistungen erforderlich seien. Tatsächlich würden zahlreiche weitere Daten gespeichert, so etwa Angaben über die verwendeten Geräte oder den Standort der benutzten Antenne und (damit) den Standort des Teilnehmers, was auch im Widerspruch zum datenschutzrechtlichen Grundsatz der Datensparsamkeit stehe, wonach Daten nur so lange und so weit gespeichert werden dürften, als dies zur Erbringung der (vertraglichen) Leistungen und zur Rechnungsstellung erforderlich sei. Betroffene könnten jedoch anhand der gesetzlichen Bestimmungen nicht ermessen, welche Daten zu welchem Zweck gespeichert würden. Dies zeige exemplarisch die Rechtsprechung des Bundesgerichts zu Antennensuchläufen. Danach dürfen Randdaten ohne Anlass, d.h. ohne dringenden Tatverdacht gegen die betroffene Person, im Rahmen eines Antennensuchlaufs etwa zum Zweck einer Rasterfahndung verwendet werden, worüber sich Betroffene gestützt allein auf die (formellgesetzlichen) Bestimmungen kaum im Klaren sein dürften. Angesichts dieser Umstände bzw. der Schwere des Grundrechtseingriffs sei die Vorinstanz zu Unrecht davon ausgegangen, es liege eine hinreichende formell-gesetzliche Grundlage für das anlasslose Speichern und Aufbewahren von Randdaten der Telekommunikation beinahe der gesamten Bevölkerung vor.

Die Beschwerdeführer stellen im Weiteren (sinngemäss) in Abrede, dass an der anlasslosen Speicherung der Randdaten ein öffentliches Interesse besteht und die Speicherung geeignet ist, effektiv einen Betrag zur Strafverfolgung zu leisten. Es bestünden andere Möglichkeiten, eine (rückwirkende) Überwachung zu ermöglichen, etwa das sog. quick freeze, bei welchem Randdaten erst bei aufkommenden dringendem Tatverdacht gespeichert würden. Solche Möglichkeiten der Überwachung seien – auch in Nachachtung des Verbots, Daten auf Vorrat zu sammeln – als milderes Mittel der anlasslosen Speicherung von Randdaten der gesamten Telekommunikation vorzuziehen; die Speicherung von Randdaten sei auf solche zu beschränken, die in einem engen zeitlichen und sachlichen Zusammenhang mit der zu untersuchenden Straftat anfielen. Und schliesslich sei

der Eingriff in das Fernmeldegeheimnis und die Meinungsfreiheit auch nicht zumutbar. Die Beschwerdeführer verweisen hierzu insbesondere auf die grosse Menge an Randdaten, welche etwa bei der Verwendung von Apps anfielen und die Möglichkeit, Randdaten mit anderen Daten zu verknüpfen. Damit liessen sich detaillierte (Bewegungs-)Profile erstellen, welche auch Rückschlüsse auf den Inhalt der Kommunikation ermöglichen würden. Der Grundrechtseingriff wiege aus diesem Grund schwer, umso mehr, als mit der Speicherung und allfälligen Erhebung von Randdaten der Grundsatz der Zweckbindung der Daten – Randdaten dienten allein dazu, die Kommunikation überhaupt erst zu ermöglichen – missachtet und das strafprozessuale nemo-tenetur-Prinzip verletzt werde. Zudem sei die Datensicherheit wie etwa ein hinreichender Schutz vor Missbrauch der Daten durch die Anbieterinnen selbst nicht gewährleistet. Insgesamt stehe somit der Nutzen der Speicherung von Randdaten für die Strafverfolgung in einem (offensichtlichen) Missverhältnis zur damit verbundenen Grundrechtseinschränkung, weshalb die Anbieterinnen anzuweisen seien, gespeicherte Randdaten der Beschwerdeführer zu löschen und keine Randdaten mehr zu speichern.

Die Beschwerdeführer verweisen sodann auf ein Urteil des Europäischen Gerichtshofes vom 8. April 2014, in dem dieser die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105/54; nachfolgend: Richtlinie zur Vorratsdatenspeicherung), für ungültig erklärt habe. Demnach und auch nach zwei Berichten der Vereinten Nationen (UNO) stelle die anlasslose Speicherung von Randdaten einen schweren Eingriff in die Grundrechte dar; die Möglichkeit, dass Kommunikationsgeheimnisse erfasst würden, erzeuge einen Eingriff in die Privatsphäre und habe einen potentiell abschreckenden Effekt, etwa seine Meinung frei zu äussern (sog. Chilling Effect). Sie müsse sich aus diesem Grund auf eine präzise gesetzliche Grundlage stützen können und auf das zur Bekämpfung schwerer Kriminalität Notwendigste beschränkt sein. Die Herausgabe von Randdaten bedürfe zudem einer vorgängigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle. Schliesslich müsse gewährleistet sein, dass auf Vorrat gespeicherte Randdaten effektiv vor Missbrauch geschützt und nach Ablauf der Speicherungsfrist unwiderruflich gelöscht würden. Diesen Anforderungen vermag nach Ansicht der Beschwerdeführer die schweizerische Regelung nicht zu genügen. Zwar schreibe die StPO vor, dass die Herausgabe von

Randdaten – abgesehen von den Randdaten der Internetnutzung – der Genehmigung durch das Zwangsmassnahmengericht bedürfe, es würden jedoch ohne Anlass die Randdaten der gesamten Telekommunikation gespeichert. Zudem sei die Datensicherheit – etwa der Schutz vor einem unberechtigten Zugriff Dritter auf die Daten – nicht gewährleistet und gespeicherte Randdaten müssten nach Ablauf der Frist von sechs Monaten nicht unwiderruflich gelöscht werden.

Zwei der Beschwerdeführer rügen ergänzend eine Verletzung der Medienfreiheit, da im Zusammenhang mit der Speicherung und Herausgabe von Randdaten das Berufsgeheimnis bzw. der Quellenschutz nicht in hinreichendem Mass gewährleistet sei. Zwar habe der Quellenschutz Eingang in das Strafprozessrecht gefunden, doch sei nicht hinreichend gewährleistet, dass die Strafverfolgungsbehörden nicht doch Kenntnis von der Quelle erhielten; anders als etwa bei Rechtsanwälten, bei welchen grundsätzlich die gesamte Kommunikation in der Berufssphäre durch das Berufsgeheimnis geschützt sei, beziehe sich der Schutz bei Journalisten nur auf die Quelle, weshalb diese im Rahmen einer Aussonderung unweigerlich bekannt werde.

D.
Mit verfahrensleitender Verfügung vom 14. November 2014 vereinigt der Instruktionsrichter die Beschwerdeverfahren aus Gründen der Verfahrensökonomie und führt sie unter der Verfahrensnummer A-4941/2014 weiter.

E.
Die Vorinstanz hält mit Schreiben vom 14. Januar 2015 an ihren Erwägungen gemäss den angefochtenen Verfügungen vom 30. Juni 2014 fest und verzichtet im Übrigen auf eine Vernehmlassung. Sie beantragt entsprechend, die Beschwerden seien abzuweisen.

F.
Mit Eingabe vom 24. April 2015 ergänzen die Beschwerdeführer ihre Argumentation. Sie verweisen auf weitere ausländische Gerichtsurteile, in welchen die jeweiligen nationalen Regelungen zur Speicherung von Randdaten aufgehoben worden seien. So habe etwa ein Gericht in Holland befunden, für rückwirkende Überwachungsmassnahmen wie der Speicherung von Randdaten bedürfe es klarer, objektiver Kriterien, welche im Gesetz verankert sein müssten. Dabei sei sicherzustellen, dass eine rückwirkende

Überwachung nur bei schweren Delikten angeordnet werde. Um einen effektiven Datenschutz zu gewährleisten, müsse zudem die innerterritoriale Speicherung der Randdaten vorgeschrieben sein. Nach Ansicht der Beschwerdeführenden vermögen die schweizerischen Bestimmungen den genannten Anforderungen nicht zu genügen; nach den Bestimmungen der StPO sei eine rückwirkende Überwachung auch bei weniger schwerwiegenden Delikten möglich und die Anbieterinnen seien nicht zu einer innerterritorialen Speicherung der Randdaten verpflichtet.

Die Beschwerdeführer weisen sodann auf einen Bericht des Menschenrechtskommissars des Europarates zur Speicherung von Randdaten auf europäischer Ebene hin. Nach diesem stehe die Speicherung von Randdaten im Widerspruch insbesondere zu den Grundsätzen der Datensparsamkeit und – mangels Verpflichtung, die Daten innerterritorial zu speichern – der Datensicherheit. Zudem werde kritisiert, dass sich die Effektivität der Speicherung von Randdaten bzw. rückwirkender Überwachungsmassnahmen nicht belegen lasse. Beides, die Verletzung datenschutzrechtlicher Grundsätze und der fehlende Nachweis der Effektivität rückwirkender Überwachungsmassnahmen, gilt nach Ansicht der Beschwerdeführenden auch mit Blick auf die schweizerischen Bestimmungen über die Speicherung und Aufbewahrung von Randdaten bzw. die Anordnung nachträglicher Überwachungsmassnahmen; in der Schweiz existiere keine Statistik bezüglich der Wirksamkeit rückwirkender Überwachungsmassnahmen und es sei auch nicht bekannt, innert welcher Frist nach Ermittlungsbeginn rückwirkende Überwachungen in der Regel angeordnet würden.

G.

Mit Zwischenverfügung vom 6. Mai 2015 weist der Instruktionsrichter ein Gesuch der Beschwerdeführer B._____ und D._____ vom 2. Februar 2015, es seien ihre Beschwerdeverfahren zu sistieren, ab, da keine hinreichenden Gründe für eine Trennung der Beschwerdeverfahren und die anbegehrte Sistierung von zwei der sechs Beschwerdeverfahren ersichtlich seien.

H.

Die Beschwerdeführenden reichen dem Bundesverwaltungsgericht am 23. Februar 2016 eine Eingabe Dritter vom 6. November 2015 an das Bundesverfassungsgericht der Bundesrepublik Deutschland ein. Diese stützt nach Ansicht der Beschwerdeführer ihre Kritik an der Speicherung von Randdaten gestützt auf das BÜPF. Insbesondere stellen sie die Effektivität

der richterlichen Überprüfung (nachträglicher) Überwachungsmassnahmen durch ein Zwangsmassnahmengericht in Frage und beantragen (aus diesem Grund) in verfahrensrechtlicher Hinsicht neu, es sei "die Praxis der Anordnung von Zwangsmassnahmen in Form der Nutzung [von] Vorratsdaten in der Schweiz und insbesondere die Praxis der richterlichen Überprüfung der beantragten Massnahmen in der Schweiz zu evaluieren". Hierzu liess sich die Vorinstanz am 23. März 2016 vernehmen und erklärte die erwähnte Eingabe als nicht einschlägig.

I.
Auf die weiteren Vorbringen der Parteien und die bei den Akten liegenden Schriftstücke wird, soweit für den Entscheid erheblich, im Rahmen der nachfolgenden Erwägungen eingegangen.

Das Bundesverwaltungsgericht zieht in Erwägung:

1.
Das Bundesverwaltungsgericht beurteilt nach Art. 31 des Verwaltungsgerichtsgesetzes (VGG, SR 173.32) Beschwerden gegen Verfügungen nach Art. 5 des Verwaltungsverfahrensgesetzes (VwVG, SR 172.021), soweit diese von einer Vorinstanz i.S.v. Art. 33 VGG erlassen worden sind und kein Ausnahmegrund i.S.v. Art. 32 VGG vorliegt.

Die Vorinstanz ist administrativ dem Eidgenössischen Justiz- und Polizeidepartement (EJPD) zugewiesen (Art. 3 Abs. 1 der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs [VÜPF, SR 780.11]). Sie gehört mithin zu den Dienststellen der Bundesverwaltung i.S.v. Art. 33 Bst. d VGG und ihre Verfügungen vom 30. Juni 2014 stellen zulässige Anfechtungsobjekte dar. Da zudem kein Ausnahmegrund vorliegt, ist das Bundesverwaltungsgericht zur Beurteilung der vorliegenden Beschwerden grundsätzlich sachlich wie funktional zuständig; es ist insbesondere nicht ersichtlich und wird auch nicht geltend gemacht, dass die Speicherung und Aufbewahrung von Randdaten der Telekommunikation den Bereich der inneren oder äusseren Sicherheit des Landes i.S.v. Art. 32 Abs. 1 Bst. a VGG betrifft und somit eine Beschwerde grundsätzlich ausgeschlossen wäre (vgl. hierzu MARTIN SIGRIST, Staatsschutz oder Datenschutz?, 2014, S. 186 ff.; zudem und auch zur Gegenausnahme BGE 138 I 6 E. 1.3.2).

Vorliegend fällt allerdings in Betracht, dass nicht die Vorinstanz, sondern die jeweiligen privaten Anbieterinnen, zu denen die Beschwerdeführer eine vertragliche Beziehung haben, die Randdaten der Telekommunikation der Beschwerdeführer speichern. Es fragt sich daher, ob die Vorinstanz sachlich und funktional zuständig war, die streitbetroffenen Verfügungen zu erlassen und den Beschwerdeführern (somit) der verwaltungsrechtliche Rechtsweg offen steht oder ob die Beschwerdeführer auf den privatrechtlichen Rechtsweg zu verweisen gewesen wären. Dies ist – wie auch das Vorliegen der übrigen Sachurteilsvoraussetzungen – im Folgenden von Amtes wegen zu prüfen (THOMAS FLÜCKIGER, in: Praxiskommentar VwVG, 2. Aufl. 2016, Art. 7 Rz. 24 mit Hinweisen; vgl. auch BGE 127 V 1 E. 1a mit Hinweisen).

Zuständigkeit der Vorinstanz

2.

2.1 Um zu beurteilen, ob eine Streitigkeit öffentlich- oder privatrechtlicher Natur ist und entsprechend gegen einen Entscheid der privat- oder der verwaltungsrechtliche Rechtsweg offen steht, ist mit Blick auf das Legalitätsprinzip in erster Linie auf die vom Gesetzgeber spezialgesetzlich vorgegebene Lösung abzustellen. Hierzu ist die betreffende Regelung auszulegen. Führt dies zu keinem (klaren) Ergebnis, ist auf die verschiedenen, in der Praxis entwickelten Kriterien zur Abgrenzung der privat- und verwaltungsrechtlichen Natur einer Bestimmung zurückzugreifen. Diese sind im Sinne einer wertenden Abwägung sachbezogen und pragmatisch miteinander zu kombinieren, um eine verlässliche Aussage über die Rechtsnatur der Norm bzw. des dieser zugrunde liegenden Rechtsverhältnisses machen zu können (Urteil des BGer 2C_386/2014, 2C_394/2014 vom 18. Januar 2016 E. 2). Dabei ist insbesondere zu berücksichtigen, ob der betreffende Rechtssatz ausschliesslich oder zumindest hauptsächlich öffentlichen oder privaten Interessen dient (Interessenkriterium), er die Erfüllung öffentlicher Aufgaben oder die Ausübung einer öffentlichen Tätigkeit regelt (Funktionskriterium), das Rechtsverhältnis einseitig durch öffentliches Recht geregelt ist und der Private in einem Subordinationsverhältnis zum Staat bzw. zur handelnden Organisation steht (Subordinationskriterium) oder die Verletzung einer Norm eine zivilrechtliche oder eine öffentlich-rechtliche Sanktion wie etwa eine Verwaltungsstrafe zur Folge hat (modales Kriterium; zum Ganzen BGE 138 II 134 E. 4 mit Hinweisen sowie Urteil des BGer 2C_386/2014, 2C_394/2014 vom 18. Januar 2016 E. 2 mit Hinweisen, insbesondere auf WIEDERKEHR/RICHLI, Praxis des Allgemeinen Verwaltungsrechts, Band I, 2012, Rz. 1 ff.).

2.2 Die Pflicht zur Speicherung und Aufbewahrung von Randdaten der Telekommunikation, wie sie vorliegend in Frage steht, findet ihre gesetzliche Grundlage im BÜPF. Dieses gilt für die Überwachung des Post- und Fernmeldeverkehrs im Rahmen von Strafverfahren, zum Vollzug von Rechtshilfeersuchen sowie im Rahmen der Suche und Rettung vermisster Personen (Art. 1 Abs. 1 BÜPF). Die (nachträgliche) Überwachung des Post- und Fernmeldeverkehrs ist demnach und nach den Ausführungen in den Materialien insbesondere ein Mittel der Strafverfolgung. Sie dient etwa der Fahndung nach Personen und der Beweissicherung, aber auch der Verhinderung von Straftaten (vgl. BGE 142 IV 34 E. 4.3.1); in Strafverfahren haben Informationen über die am Fernmeldeverkehr beteiligten Personen, die Art und Dauer der Verbindung sowie den Standort der Fernmeldeanlage eine fast ebenso grosse Bedeutung wie die Kenntnis der übermittelten Nachrichten (zum Ganzen Botschaft des Bundesrates vom 1. Juli 1998 zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung, BBl 1998 IV 4241, 4256 f., 4259 sowie 4268, nachfolgend: Botschaft BÜPF). Die Anbieterinnen sind aus diesem Grund verpflichtet, die Randdaten während sechs Monaten aufzubewahren und sie der Vorinstanz auf deren Verlangen hin zuzuleiten (Art. 15 Abs. 1 und 3 BÜPF). Diese nimmt die Daten von den Anbieterinnen entgegen und leitet sie an die anordnende Strafverfolgungsbehörde weiter (Art. 13 Abs. 1 Bst. e BÜPF). Die Vorinstanz kann die Anbieterinnen zudem anweisen, die für die Überwachung notwendigen (technischen) Massnahmen zu treffen (Art. 13 Abs. 1 Bst. b BÜPF). Eine entsprechende Befugnis kommt der Vorinstanz auch losgelöst von einer konkreten Überwachung zu (BVGE 2009/46 E. 7.4). Gegen Verfügungen der Vorinstanz steht den Anbieterinnen die Beschwerde an das Bundesverwaltungsgericht offen, soweit sie etwa geltend machen, sie seien zur Ausführung einer Übermittlungsanordnung aus technischen oder organisatorischen Gründen nicht im Stande (vgl. Art. 32 VÜPF; BVGE 2009/46 E. 3, insbes. E. 3.3.2; vgl. kritisch zu den Rechtsgrundlagen sowie zur Rechtsprechung betreffend die Beschwerdelegitimation und die zulässigen Beschwerdegründe bzw. die Überprüfungsbefugnis von Vorinstanz und Bundesverwaltungsgericht ANDREAS HEINIGER, Schrankenlose Fernmeldeüberwachung aufgrund eines konzeptionellen Fehlers im BÜPF?, Jusletter vom 17. September 2012, insbes. Rz. 26–35).

2.3 Darüber, welchem Recht die streitbetroffene Pflicht zur Speicherung von Randdaten der Telekommunikation zugehörig ist und welcher Rechtsweg den Betroffenen offen steht, lässt sich den gesetzlichen Bestimmun-

gen von BÜPF und VÜPF wie auch den Materialien unmittelbar nichts entnehmen. Es ist daher – wie vorstehend ausgeführt – auf die weiteren, in der Rechtsprechung entwickelten Kriterien zurück zu greifen, um zu bestimmen, welchem Recht die vorliegende Streitigkeit untersteht.

Die Speicherung und Aufbewahrung von Randdaten ist – soweit sie vorliegend in Frage steht (vgl. zum Streitgegenstand nachfolgend E. 4) – nicht Selbstzweck, sondern dient, wie vorstehend ausgeführt, insbesondere der Strafverfolgung. Letztere ist, dem gesetzlich verankerten Grundsatz des staatlichen Straf- und Justizmonopols entsprechend, alleinige Aufgabe des Staates (Art. 2 Abs. 1 StPO; STRAUB/WELTERT, in: Basler Kommentar zur StPO, 2. Aufl. 2014, Art. 2 StPO Rz. 1). Aus dem Grundsatz des staatlichen Strafmonopols folgt sodann der Untersuchungsgrundsatz, wonach die Strafverfolgungsbehörden den massgeblichen Sachverhalt von Amtes wegen abzuklären und hierfür alle notwendigen Beweise zu erheben haben (Art. 6 Abs. 1 StPO; STRAUB/WELTERT, a.a.O., Art. 2 StPO Rz. 3; WOLFGANG WOHLERS, in: Donatsch/Hansjakob/Lieber, Kommentar zur Schweizerischen Strafprozessordnung [StPO], 2. Aufl. 2014, Art. 6 Rz. 5). Sie haben die belastenden und entlastenden Umstände mit gleicher Sorgfalt zu untersuchen (Art. 6 Abs. 2 StPO). Die Abklärung aller bedeutsamen Tatsachen – und damit u.a. auch die Speicherung und Aufbewahrung von Randdaten als (potentiell be- und entlastende) Beweise durch die Anbieterinnen – ist somit Aufgabe des Staates, jedenfalls soweit wie vorliegend offenbar Daten gespeichert und länger aufbewahrt werden, als dies für die Erbringung der vertraglichen Leistungen erforderlich wäre (vgl. TPF 2011 42 E. 4.2.1 b; zudem MÜLLER/SCHEFER, Grundrechte in der Schweiz, 4. Aufl. 2008, S. 208, wonach die privaten Anbieterinnen mit der Speicherung und Aufbewahrung von Randdaten eine staatliche Aufgabe wahrnehmen und nach Art. 35 Abs. 2 BV ebenfalls an die Grundrechte gebunden sind; hierzu auch EVA MARIA BELSER, in: Belser/Epiney/Waldmann [Hrsg.], Datenschutzrecht, 2011, § 6 Rz. 108). Unter dem Blickwinkel des Funktionskriteriums ist die Speicherung und Aufbewahrung von Randdaten somit als öffentliche Aufgabe des Bundes zu qualifizieren (zur Auslagerung polizeilicher Aufgaben vgl. GIOVANNI BIAGGINI, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 178 Rz. 28).

An der Strafverfolgung sowie der Suche und Rettung vermisster Personen besteht sodann in einem Rechtsstaat ein erhebliches öffentliches Interesse. Die gesetzliche Pflicht, die Randdaten der Telekommunikation zu speichern und während sechs Monaten aufzubewahren, dient somit haupt-

sächlich öffentlichen Interessen (Interessenkriterium) und es steht den Anbieterinnen sowie den Beschwerdeführern mit Blick auf die gesetzliche Regelung in Art. 15 Abs. 1 und 3 BÜPF nicht frei, Speicherung und Aufbewahrung der Randdaten sowie deren allfällige Herausgabe abweichend zu regeln bzw. Abweichendes zu vereinbaren (Subordinationskriterium).

Insgesamt ist somit davon auszugehen, dass die Streitsache, d.h. die Pflicht zur Speicherung und Aufbewahrung der Randdaten der Telekommunikation der Beschwerdeführer, in einen vom öffentlichen Recht geregelten Bereich fällt bzw. dem öffentlichen Recht unterstellt ist. Damit steht den Beschwerdeführern grundsätzlich der verwaltungsrechtliche Rechtsmittelweg offen. Die Vorinstanz hat sie insofern zu Recht nicht auf den privatrechtlichen Rechtsweg verwiesen. An dieser Beurteilung vermag der Umstand, dass die betreffenden Randdaten naturgemäss bei den privaten Anbieterinnen anfallen und die Anbieterinnen aufgrund dieser Sachnähe verpflichtet sind, Randdaten zu speichern und aufzubewahren, für sich alleine nichts zu ändern.

Das Ergebnis ist auch sachgerecht. Wie vorstehend erwogen, ist das Verhältnis zwischen der Vorinstanz und den Anbieterinnen unstreitig verwaltungsrechtlicher Natur und steht den Anbieterinnen gegen Verfügungen bzw. aufsichtsrechtliche Anordnungen der Vorinstanz der verwaltungsrechtliche Rechtsweg offen (vgl. vorstehend E. 2.2). Dies muss – vorbehältlich einer abweichenden spezialgesetzlichen Regelung – auch für die Pflicht zur Speicherung von Randdaten im Verhältnis zwischen den Anbieterinnen und betroffenen Personen gelten. Stünde betroffenen Personen hinsichtlich der Speicherung und Aufbewahrung ihrer Randdaten durch die Anbieterinnen ein anderer, d.h. privatrechtlicher Rechtsmittelweg offen, so verbliebe grundsätzlich gleichwohl die Möglichkeit, die Vorinstanz zusätzlich aufsichtsrechtlich anzurufen. Indem betroffenen Personen der verwaltungsrechtliche Rechtsweg offen steht, kann also vermieden werden, dass das Rechtsmittel und Rechtsbehelf auseinanderfallen bzw. die Speicherung und Aufbewahrung von Randdaten der Telekommunikation sowohl privat- als auch verwaltungsrechtlich gerügt und geprüft werden kann (vgl. in diesem Sinn das Urteil des BGer 2C_386/2014, 2C_394/2014 vom 18. Januar 2016 E. 7.4.2). Sich widersprechende Entscheide können so vermieden werden. Zwar ist wie gesagt an sich nicht ausgeschlossen, den Rechtsschutz spezialgesetzlich anders zu gestalten. Hierzu bedürfte es indes einer hinreichend bestimmten gesetzlichen Grundlage, die vorliegend jedoch nicht vorhanden ist.

2.4

2.4.1 Im Hinblick auf die Zuständigkeit der Vorinstanz ist sodann zu prüfen, ob mit der Übertragung einer öffentlichen Aufgabe – der Speicherung und Aufbewahrung von Randdaten – an die Anbieterinnen (implizit) auch hoheitliche Befugnisse, konkret Verfügungsbefugnisse, auf die Anbieterinnen übertragen wurden.

2.4.2 Das VwVG findet nach dessen Art. 1 Abs. 1 Anwendung auf Verfahren in Verwaltungssachen, die durch Verfügungen von Bundesverwaltungsbehörden zu erledigen sind. Zu den Behörden zählen auch Instanzen oder Organisationen ausserhalb der Bundesverwaltung, soweit sie in Erfüllung ihnen übertragener öffentlich-rechtlicher Aufgaben des Bundes verfügen (Art. 1 Abs. 2 Bst. e VwVG). Darunter können sowohl private als auch öffentlich-rechtliche Organisationen und Personen wie etwa juristische Personen des Privatrechts fallen (NADINE MAYHALL, in: Praxiskommentar VwVG, 2. Aufl. 2016, Art. 1 Rz. 30; vgl. auch das Urteil des BGer 2C_386/2014, 2C_394/2014 vom 18. Januar 2016 E. 5.1). Die Generalklausel von Art. 1 Abs. 2 Bst. e VwVG erfasst somit grundsätzlich alle nicht unmittelbar dem Staat zuzurechnenden Instanzen, welche Verwaltungsaufgaben des Bundes erfüllen und denen die Befugnis zum Erlass von Verfügungen zukommt.

Die Befugnis, Verfügungen gemäss Art. 5 VwVG zu erlassen, d.h. im Anwendungsfall eine verbindliche Regelung eines Rechtsverhältnisses zu definieren, die einseitig Rechte und Pflichten berührt, ist ein Souveränitätsprivileg der Behörden. Gleich wie die Übertragung einer öffentlichen Aufgabe bedarf auch die Übertragung von Verfügungsbefugnissen an eine ausserhalb der Bundesverwaltung stehende Organisation oder Person einer hinreichenden formell-gesetzlichen Grundlage (BGE 138 II 134 E. 5.1 mit Hinweisen auf die Rechtsprechung). Zwar kann die Übertragung der Aufgabe implizit auch die für die Erfüllung erforderliche Verfügungskompetenz enthalten, doch setzt dies nach der Rechtsprechung voraus, dass die gesetzliche Regelung dem nicht entgegensteht und sich die Verfügungskompetenz als zur Wahrnehmung der übertragenen Aufgabe(n) sachnotwendig erweist (Urteil des BGer 2C_386/2014, 2C_394/2014 vom 18. Januar 2016 E. 5.2; vgl. auch BGE 137 II 409 E. 6.2 und 7.4; TSCHANNEN/ZIMMERLI/MÜLLER, Allgemeines Verwaltungsrecht, 4. Aufl. 2014, § 10 Rz. 19).

2.4.3 Im Zentrum stehen die Bestimmungen von Art. 15 Abs. 1 und 3 BÜPF. Damit werden die Anbieterinnen verpflichtet, die Randdaten wäh-

rend sechs Monaten aufzubewahren und auf Verlangen der Vorinstanz zuzuleiten. Eine Bestimmung, welche den Anbieterinnen die Befugnis übertragen würde, (im Streitfall) bezüglich Speicherung, Aufbewahrung und Herausgabe von Randdaten Verfügungen zu erlassen, findet sich im Gesetz nicht. Sie lässt sich auch nicht implizit der Pflicht zur Wahrnehmung der öffentlichen Aufgabe, der Speicherung und Aufbewahrung von Randdaten der Telekommunikation, entnehmen, ist doch die Verfügungsbefugnis zur Erfüllung der (auf einen tatsächlichen Erfolg gerichteten) öffentlichen Aufgabe sachlich nicht notwendig; die Randdaten fallen bei der jeweiligen Anbieterin an und werden von dieser gespeichert und aufbewahrt. Die Anbieterinnen sind insoweit keine zum Erlass von Verfügungen befugten Behörden.

Die Vorinstanz, bei der es sich um eine Behörde handelt, hat sich demnach zu Recht als sachlich zuständig erachtet, über die Begehren der Beschwerdeführer zu entscheiden. Sie ist auf dem Gebiet der Überwachung des Post- und Fernmeldeverkehrs – was die Speicherung und Aufbewahrung sowie die Herausgabe der Daten anbelangt – allgemein (zur Aufsicht) zuständig und daher befugt, zu den im BÜPF geregelten Tatbeständen und somit auch vorliegend hinsichtlich der Rechte und Pflichten der Anbieterinnen Verfügungen zu erlassen (vgl. vorstehend E. 2.2 und nachfolgend E. 12.7.4; zudem sinngemäss Urteil des BGer 2C_715/2008 vom 15. April 2009 E. 4.4 f.). Ergänzend kann an dieser Stelle darauf hingewiesen werden, dass der Bundesrat gemäss seiner Botschaft vom 27. Februar 2013 zu einer Totalrevision des BÜPF die Zuständigkeit der Vorinstanz zur Aufsicht über den Vollzug neu im Gesetz festzuschreiben gedenkt und aus den Materialien nicht hervorgeht, dass damit eine von der bisherigen Ordnung abweichende Regelung geschaffen werden soll (Botschaft des Bundesrates vom 27. Februar 2013 zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BBl 2013 2683, 2763, nachfolgend Botschaft nBÜPF; vgl. in diesem Zusammenhang auch BVGE 2013/13 E. 5.4.3, wonach eine Abweichung vom bisherigen ordnungspolitischen Grundentscheid zumindest aus den Materialien hervorgehen müsste). Gegen die Verfügungen der Vorinstanz steht betroffenen Personen alsdann grundsätzlich der verwaltungsrechtliche Rechtsweg offen (Art. 44 VwVG).

2.4.4 Zu prüfen bleibt, ob sich allenfalls aus dem Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1) oder aus dem Fernmeldegesetz vom 30. April 1997 (FMG, SR 784.10) eine andere Zuständigkeitsordnung ergibt.

Das DSG findet grundsätzlich auch auf die Bearbeitung von Personendaten durch die Anbieterinnen Anwendung, zumal diese im Rahmen der Speicherung und Aufbewahrung von Randdaten der Telekommunikation mit der Erfüllung einer öffentlichen Aufgabe des Bundes betraut sind (Art. 2 Abs. 1 Bst. b und Art. 3 Bst. h DSG, wonach als Bundesorgane u.a. Personen gelten, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind ["la personne en tant qu'elle est chargée d'une tâche de la Confédération" gemäss dem französischen bzw. "pure persone nella misura in cui sono loro affidati compiti federali" gemäss dem italienischen Wortlaut]; vgl. auch vorstehend E. 2.3 sowie nachfolgend E. 12.7.3). Den Beschwerdeführern stehen insoweit gegenüber der verantwortlichen Behörde die Ansprüche gemäss Art. 25 DSG offen, welche darüber in Form einer anfechtbaren Verfügung zu entscheiden hat (Art. 25 Abs. 4 DSG; vgl. hierzu auch nachfolgend E. 12.7.4). Zwar folgt die datenschutzrechtliche Verantwortung in erster Linie aus der Kompetenz und Aufgabe zur Datenbearbeitung, was insofern auf die Zuständigkeit der Anbieterinnen schliessen liesse. Im Datenschutzrecht gilt jedoch das Prinzip der Spezialermächtigung (Art. 17 Abs. 1 DSG). Das DSG ist als allgemeines Datenschutzgesetz, als Rahmengesetz, konzipiert und verweist für die konkrete Datenbearbeitung auf bereichsspezifische Rechtsgrundlagen (CLAUDIA MUND, in: Baeriswyl/Pärli [Hrsg.], Datenschutzgesetz [DSG], 2015, Art. 17 Rz. 2; SARAH BALLENEGGER, in: Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, Art. 17 DSG Rz. 3). Es vermag daher originär keine Verfügungsbefugnis der Anbieterinnen bezüglich der Speicherung der Randdaten zu begründen. Zum Erlass von Verfügungen im Streitfall ist vielmehr, wie vorstehend erwogen, gestützt auf die bereichsspezifische Regelung im BÜPF die Vorinstanz zuständig. Nicht zu beanstanden ist deshalb vorliegend, dass sich die Beschwerdeführer, nachdem sie von den Anbieterinnen auf Anfrage hin keine (vollständige) Auskunft über gespeicherte Randdaten erhalten haben, hinsichtlich der vorliegend zu beurteilenden Begehren die Vorinstanz angerufen haben und diese sich als sachlich und funktional zuständig erachtet hat (vgl. diesbezüglich auch nachfolgend E. 12.7.4).

Kein abweichender Schluss ergibt sich aus dem FMG. Zwar sind die Anbieterinnen verpflichtet, das anwendbare Recht und damit auch das BÜPF einzuhalten (Art. 6 Abs. 1 Bst. b FMG) sowie das Fernmeldegeheimnis zu wahren (Art. 43 FMG); die Sicherstellung des aus der Verfassung abgeleiteten und im FMG gesetzlich verankerten Fernmeldegeheimnisses gehört zudem zu den Konzessionsbedingungen, die während der gesamten Laufzeit einzuhalten sind (FISCHER/SIDLER, in: Informations- und Kommunikationsrecht, Schweizerisches Bundesverwaltungsrecht Band V, Teil 1, 2. Aufl.

2003, Rz. 328). Eine sachliche Zuständigkeit des Bundesamtes für Kommunikation (BAKOM), dem nach Art. 58 FMG die Aufsicht über die Anbieterinnen zukommt, lässt sich (allein) damit für die vorliegende Streitsache jedoch nicht begründen. Das FMG bezweckt, dass der Bevölkerung und der Wirtschaft vielfältige, preiswerte, qualitativ hoch stehende sowie national und international konkurrenzfähige Fernmeldedienste angeboten werden (Art. 1 Abs. 1 FMG). Hierzu steht die vorliegende Streitsache bzw. stehen die Begehren der Beschwerdeführer in keinem unmittelbaren sachlichen Zusammenhang. Daran ändert nichts, dass die Beschwerdeführer eine Verletzung des grundrechtlich geschützten Fernmeldegeheimnisses rügen, zu deren Einhaltung die Anbieterinnen (auch) durch Art. 43 FMG verpflichtet werden. Sie wenden sich mit ihren Begehren explizit gegen die im BÜPF geregelte Pflicht der Anbieterinnen, die Randdaten der Telekommunikation zu speichern und während sechs Monaten aufzubewahren (Art. 15 Abs. 3 BÜPF). (Sachlicher) Anknüpfungspunkt ist somit die Überwachung des Fernmeldeverkehrs und nicht das Erbringen von Fernmeldedienstleistungen bzw. eine damit in (unmittelbarem) Zusammenhang stehende Rechtsverletzung, welche die Zuständigkeit des BAKOM i.S.v. Art. 58 FMG zu begründen vermögen würde (vgl. in diesem Sinne BGE 126 I 50 E. 2; zur Zusammenarbeit von Vorinstanz und BAKOM THOMAS HANSJAKOB, BÜPF / VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2. Aufl. 2006, Art. 2 BÜPF Rz. 10–12, nachfolgend: Kommentar BÜPF / VÜPF).

2.5 Zusammenfassend ergibt sich, dass sich die Vorinstanz zu Recht als sachlich zuständig angesehen hat, die angefochtenen Verfügungen zu erlassen. Die weiteren Sachentscheidvoraussetzungen auf Seiten der Vorinstanz geben sodann zu keinen grundsätzlichen Bemerkungen Anlass. Die Pflicht der Anbieterinnen, die Randdaten der Telekommunikation der Beschwerdeführer zu speichern und aufzubewahren, stützt sich auf öffentliches Recht des Bundes (Art. 15 Abs. 3 BÜPF) und die Beschwerdeführer machen in vertretbarer Weise geltend, dass sie hierdurch in grundrechtlich geschützten Positionen – ihren Ansprüchen auf informationelle Selbstbestimmung und Vertraulichkeit der Kommunikation – berührt sind (vgl. Urteil des BGer 2C_272/2012 vom 9. Juli 2012 E. 4.4.4–4.4.6 mit Hinweisen auf die Literatur und die Rechtsprechung; zudem analog das Urteil des BGer 1C_165/2009 vom 3. November 2009 E. 2.3 mit Hinweisen auf die Rechtsprechung; ebenso das Urteil des BVGer A-4918/2011, A-4924/2011 vom 4. Juni 2012 E. 6.2). Die Beschwerdeführer hatten daher, da im Fall der Gutheissung ihrer Begehren eine Speicherung in Zukunft unterbliebe und gespeicherte Randdaten gelöscht würden, ein schutzwürdiges Interesse

am Erlass der angefochtenen Verfügungen. Schliesslich besteht keine andere Möglichkeit, den Beschwerdeführern genügenden Rechtsschutz gegen die Speicherung und Aufbewahrung der Randdaten ihrer Telekommunikation zu gewähren (vgl. Urteil des BGer 1C_455/2011 vom 12. März 2012 E. 4.5 und 4.7). Zwar können Personen, deren Fernmeldeanschluss überwacht worden ist, hiergegen nachträglich Beschwerde nach den Art. 393–397 StPO führen (Art. 279 Abs. 3 StPO), doch setzt dies voraus, dass eine Überwachung tatsächlich angeordnet worden ist. Dieses Rechtsmittel steht vorliegend nicht zur Verfügung und ebenso wenig ist ein anderes auf Erlass einer Verfügung gerichtetes Verfahren ersichtlich, welches den Beschwerdeführern die Möglichkeit der nachträglichen Verwaltungsrechtspflege eröffnen würde. Es ist daher von einem hinreichenden Rechtsschutzbedürfnis der Beschwerdeführer auszugehen.

Die Vorinstanz ging nach dem Gesagten und auch im Sinne eines wirksamen Grundrechtsschutzes zu Recht von einem hinreichenden Rechtsschutzinteresse der Beschwerdeführer aus und ist insoweit zu Recht auf die Gesuche der Beschwerdeführer eingetreten (Urteil des BGer 2C_272/2012 vom 9. Juli 2012 E. 4.3, wonach die Anfechtbarkeit entsprechend dem verfassungsrechtlich geschützten Bedürfnis nach gerichtlicher Kontrolle konzipiert sein muss; vgl. auch BGE 138 I 6 E. 1.2; ferner BGE 130 I 369 E. 6.1 bezüglich des Anspruchs gestützt auf Art. 13 EMRK; RAINER J. SCHWEIZER, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 36 Rz. 2).

Beschwerdelegitimation

3.
Zur Beschwerde an das Bundesverwaltungsgericht ist nach Art. 48 Abs. 1 VwVG berechtigt, wer am Verfahren vor der Vorinstanz teilgenommen hat, durch die angefochtene Verfügung besonders berührt ist und ein schutzwürdiges Interesse an deren Aufhebung oder Änderung hat. Verlangt ist somit nebst der formellen Beschwer, dass der Beschwerdeführer über eine besondere Beziehungsnähe zur Streitsache verfügt und einen praktischen Nutzen aus der Aufhebung oder Änderung der angefochtenen Verfügung zu ziehen vermag. Davon ist vorliegend auszugehen; die Beschwerdeführer sind mit ihren Begehren – soweit die Vorinstanz darauf überhaupt eingetreten ist – nicht durchgedrungen. Sie sind daher als zur Beschwerdeerhebung berechtigt anzusehen.

Streitgegenstand

4.

4.1 Der Streitgegenstand des Beschwerdeverfahrens bestimmt sich nach dem in der angefochtenen Verfügung geregelten Rechtsverhältnis und den Parteibegehren. Streitgegenstand ist entsprechend das in der angefochtenen Verfügung geregelte Rechtsverhältnis, soweit es im Streit liegt (JÉRÔME CANDRIAN, Introduction à la procedure administrative fédérale, 2013, N. 182).

Das Rechtsverhältnis ergibt sich aus dem Dispositiv der angefochtenen Verfügung. Bestehen Zweifel über die genaue Tragweite der im Dispositiv geregelten Rechte und Pflichten, ist auf die Begründung der Verfügung zurückzugreifen. Gleiches gilt in Bezug auf die Parteibegehren. Lässt das Rechtsbegehren nicht deutlich erkennen, in welchem Sinne die Verfügung abgeändert werden soll, ist auf die Begründung zurückzugreifen, um zu ermitteln, was Streitgegenstand ist. Dieser ergibt sich stets aus der beantragten Rechtsfolge. Gegenstand des Beschwerdeverfahrens kann schliesslich nur sein, was Gegenstand des vorinstanzlichen Verfahrens war. Streitfragen, über welche die Vorinstanz nicht verfügt hat, darf die Beschwerdeinstanz nicht beurteilen, da sie ansonsten in die funktionale Zuständigkeit der Vorinstanz eingreifen würde. Auf entsprechende Parteibegehren kann nicht eingetreten werden. Liegt ein Nichteintretensentscheid vor, können demnach im Beschwerdeverfahren keine Begehren in der Sache selbst gestellt werden. Lediglich die formelle Prüfung der Vorinstanz kann in diesen Fällen Gegenstand der materiellen Beurteilung durch die Beschwerdeinstanz sein (zum Ganzen Urteil des BVGer A-2332/2014 vom 18. Januar 2016 E. 1.3.1 mit Hinweisen; vgl. zudem Urteil des BGer 2C_272/2012 vom 9. Juli 2012 E. 1.1).

4.2

4.2.1 Die Vorinstanz hat die Begehren der Beschwerdeführer abgewiesen, soweit diese verlangt hatten, es seien die Anbieterinnen anzuweisen, gespeicherten Randdaten zu löschen und deren Speicherung in Zukunft zu unterlassen (Antrag Ziff. 1 gemäss den Schreiben vom 20. Februar 2014). Insofern liegt ein Sachentscheid vor und ist Streitgegenstand des vorliegenden Verfahrens, ob die Vorinstanz die genannten Begehren der Beschwerdeführer zu Recht abgewiesen hat.

4.2.2 Präzisiert werden muss, auf welche Daten sich die Rechtsbegehren der Beschwerdeführer konkret beziehen. Diese verlangen nach Ziff. 2 ihrer

Anträge, es seien "die gemäss Art. 15 Abs. 3 BÜPF gespeicherten Verkehrs- und Rechnungsdaten" zu löschen und die Speicherung in Zukunft zu unterlassen. In der Beschwerdebegründung sprechen sie sodann von "Metadaten" und beziehen sich dabei auf die Daten gemäss Art. 15 Abs. 3 BÜPF. Nach dem Wortlaut des erwähnten Art. 15 Abs. 3 BÜPF sind die Anbieterinnen verpflichtet, *die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten* zu speichern und während sechs Monaten aufzubewahren. Dabei setzt die Pflicht zur Aufbewahrung unstrittig die vorgängige Speicherung der betreffenden Daten voraus. Darauf ist näher einzugehen.

Das Gesetz unterscheidet bei der Überwachung des Fernmeldeverkehrs grundsätzlich zwischen der *Auskunft über sog. Bestandesdaten* (Art. 14 BÜPF), *der (rückwirkenden) Erhebung von Daten zur Teilnehmeridentifikation sowie von Verkehrs- und Rechnungsdaten* (Art. 15 Abs. 1 und 3 BÜPF, Art. 273 Abs. 1 StPO) und der *inhaltlichen Überwachung des Fernmeldeverkehrs* (Art. 15 Abs. 1 BÜPF, Art. 269 StPO). Wesentlich ist somit, ob sich die Überwachung auf den *Inhalt* des Fernmeldeverkehrs (Call Content) oder die mit dem Fernmeldeverkehr verbundenen Informationen (Intercept Related Information [IRI], sog. *Randdaten* bzw. äussere Daten des Kommunikationsvorgangs) bezieht oder lediglich um Auskunft über *Bestandesdaten* ersucht wird.

Zur Unterscheidung von Rand- und Bestandesdaten ist Folgendes wesentlich: Als Bestandesdaten gelten Daten, die unabhängig von einem bestimmten Fernmeldeverkehr unveränderlich vorhanden sind. Wird um Auskunft über Bestandesdaten ersucht, ist der Fernmeldeanschluss – etwa eine Rufnummer oder eine IP-Adresse – bereits bekannt und es wird den auskunftsberechtigen Behörden einzig mitgeteilt, wer als Inhaber bzw. Rechnungsadressat dieses Anschlusses bei der Anbieterin registriert ist (Art. 14 Abs. 1 und 4 BÜPF sowie Art. 19 Abs. 1 und Art. 27 Abs. 1 VÜPF; THOMAS HANSJAKOB, in: Donatsch/Hansjakob/Lieber [Hrsg.], Kommentar zur Schweizerischen Strafprozessordnung [StPO], 2. Aufl. 2014, Art. 272 Rz. 4, nachfolgend: Kommentar StPO). Es geht um die Beantwortung der Frage, wer einen bestimmten Fernmeldeanschluss benutzt (hat) bzw. welcher Person eine der anfragenden Behörde bekannte Telefonnummer oder IP-Adresse zugeordnet ist. Diese Angaben betreffen nicht den Fernmelde*verkehr*, sondern stehen lediglich im Zusammenhang mit Fernmelde*anschlüssen*, weshalb auch eine vorgängige richterliche Genehmigung nicht erforderlich ist.

Demgegenüber soll die (rückwirkenden) Erhebung von Randdaten aufzeigen, mit wem eine bestimmte verdächtige Person in der fraglichen Zeitperiode wann und wie lange kommuniziert hat. Sie beschlägt entsprechend und im Unterschied zur blossen Auskunft über Bestandesdaten konkrete Fernmeldebeziehung(en) und bedarf als Überwachungsmassnahme einer richterlichen Genehmigung (zum Ganzen BGE 141 IV 108 E. 5.1 und E. 6.2 sowie Urteil des BGer 1B_265/2012 vom 21. August 2012 E. 2.1; HANSJAKOB, Kommentar StPO, Art. 273 Rz. 3 f. und 7 f. mit Hinweisen; THOMAS HANSJAKOB, Wichtige Entwicklungen der Bundesgerichtspraxis zur Überwachung des Post- und Fernmeldeverkehrs, forumpoenale 2013 S. 173 ff., S. 176 f., nachfolgend: Bundesgerichtspraxis; zudem MARC JEAN-RICHARD-DIT-BRESSEL, in: Basler Kommentar zur StPO, 2. Aufl. 2014, Art. 273 Rz. 7).

Die Begriffe betreffend die zu speichernden und aufzubewahrenden Daten werden in der Rechtsprechung und der Lehre nicht einheitlich verwendet und auch aus dem BÜPF sowie aus der StPO ergibt sich die vorstehend dargestellte Terminologie nicht auf den ersten Blick. Sie ist jedoch geltendes Recht, wie die Materialien zur Totalrevision des BÜPF zeigen. Nach diesen wird die Erwähnung der Verkehrs- und Rechnungsdaten – und auch der Daten zur Teilnehmeridentifikation – aufgehoben und neu der Begriff "Randdaten" verwendet, ohne dass sich der materielle Inhalt des Begriffs ändert (Botschaft nBÜPF, BBl 2013 2683, 2739; vgl. zur Berücksichtigung der Materialien zur Totalrevision des BÜPF auch nachfolgend E. 7.3.3). Was unter Randdaten zu verstehen ist, wird neu im Gesetz selbst umschrieben. Als Randdaten gelten demnach 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 (Art. 8 Bst. b des Entwurfs zu einem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF], BBl 2013 2789, 2791). Vorliegend wird daher – im Sinne auch einer geltungszeitlichen Auslegung – von diesem Begriffsverständnis ausgegangen und – wie bereits vorstehend – für alle Daten, welche gestützt auf Art. 15 Abs. 3 BÜPF von den Anbietern zu speichern und aufzubewahren sind, der Begriff "Randdaten" verwendet. Diese sind wie erwähnt abzugrenzen vom Inhalt der Kommunikation und den Bestandesdaten.

4.2.3 Die Beschwerdeführer beschränken ihre Rechtsbegehren dem Wortlaut nach auf die Verkehrs- und Rechnungsdaten. Unter Berücksichtigung der Beschwerdebegründungen ist jedoch davon auszugehen, dass sie sich

umfassend gegen die Speicherung von Randdaten ihrer Telekommunikation – die Beschwerdeführer bezeichnen diese in ihrer Beschwerdebegründung wie bereits erwähnt als "Metadaten" bzw. "Vorratsdaten", wobei diese Begriffe im schweizerischen Recht nicht gebräuchlich sind – zur Wehr setzen, jedenfalls soweit die betroffenen Daten nicht für die Erbringung der vertraglichen Leistungen zwingend erforderlich sind. Streitgegenstand ist somit die Frage, ob die Speicherung und Aufbewahrung von Randdaten der Telekommunikation der Beschwerdeführer durch die Anbieterinnen zulässig ist.

Nicht Streitgegenstand ist demgegenüber die Frage, ob die Erteilung von Auskünften über Bestandesdaten wie Name, Adresse und Beruf des Teilnehmers in einem vereinfachten Verfahren zulässig bzw. mit den Grundrechten der Beschwerdeführer, insbesondere mit dem Anspruch auf Schutz vor Missbrauch persönlicher Daten (vgl. BGE 133 IV 271 E. 2.5; Urteil des BGer 1C_74/2015 vom 2. Dezember 2015 E. 4.1), vereinbar ist; die Beschwerdeführer wenden sich weder in ihren Rechtsbegehren noch in ihrer Beschwerdebegründung gegen die Herausgabe von Bestandesdaten i.S.v. Art. 14 (Abs. 1) BÜPF (zur Mitteilung von Bestandesdaten in einem vereinfachten Verfahren KESSLER/ISENRING, Die geplante Total-Revision des BÜPF im Überblick, in: Sicherheit & Recht 1/2011 S. 30).

4.3 Auf den Antrag der Beschwerdeführer, es seien die Anbieterinnen zu verpflichten, keine Randdaten an die Vorinstanz oder an andere Behörden oder Gerichte herauszugeben (Antrag Ziff. 2), ist die Vorinstanz nicht eingetreten. Gegenstand der Beurteilung durch das Bundesverwaltungsgericht kann daher diesbezüglich nur die formelle Prüfung der Vorinstanz bzw. die Frage sein, ob die Vorinstanz auf den Antrag der Beschwerdeführer zu Recht nicht eingetreten ist. Eine Gutheissung könnte einzig zur Folge haben, dass die Vorinstanz nach einer Rückweisung über die gestellten Begehren materiell entscheiden müsste. Soweit die Beschwerdeführer darüber hinaus in der Sache (erneut) verlangen, es seien die Anbieterinnen anzuweisen, keine gespeicherten Randdaten an die Vorinstanz oder an eine andere Behörde oder ein Gericht herauszugeben, liegt eine unzulässige Ausweitung des Streitgegenstandes vor und kann auf die Beschwerden nicht eingetreten werden.

5.

Auf die im Übrigen frist- und formgerecht eingereichte Beschwerde (Art. 50 Abs. 1 und Art. 52 Abs. 1 VwVG) ist demnach vorbehältlich der Einschränkung gemäss vorstehend E. 4.3 einzutreten

Kognition

6.
Das Bundesverwaltungsgericht überprüft die angefochtenen Verfügungen auf Verletzung von Bundesrecht – einschliesslich der unvollständigen oder unrichtigen Feststellung des rechtserheblichen Sachverhalts und Rechtsfeh-ler bei der Ausübung des Ermessens – sowie auf Angemessenheit (Art. 49 VwVG). Es auferlegt sich grundsätzlich eine gewisse Zurückhaltung, wenn technische Fragen zu beurteilen sind oder die Vorinstanz gestützt auf die ihr vom Gesetzgeber beigegebenen Fachbehörden entschieden hat (BVGE 2011/33 E. 4.4 mit Hinweisen; CANDRIAN, a.a.O., N. 191). Voraussetzung für diese Zurückhaltung ist, dass im konkreten Fall keine Anhaltspunkte für eine unrichtige oder unvollständige Sachverhaltsfeststellung vorliegen und davon ausgegangen werden kann, die Vorinstanz habe die für den Entscheid wesentlichen Gesichtspunkte geprüft und die erforderlichen Abklärungen sorgfältig und umfassend vorgenommen (Urteil des BVGer A-2575/2013 vom 17. September 2014 E. 2; vgl. zudem Urteil des BVGer A-1251/2012 vom 15. Januar 2014 E. 6.3.3).

Einzugehen ist sodann auf die Bestimmung von Art. 190 BV, die Bundesgesetze und Völkerrecht für das Bundesgericht und die anderen rechtsanwendenden Behörden – und somit auch für das Bundesverwaltungsgericht – für massgebend erklärt. Demnach ist es den rechtsanwendenden Behörden verboten, Bundesgesetze und Völkerrecht in einem konkreten Streitfall die Anwendung mit dem Argument zu versagen, sie seien verfassungswidrig. Die Bestimmung statuiert jedoch kein Prüfungsverbot, sondern bewirkt ein Anwendungsgebot (BGE 140 I 353 E. 4.1; vgl. auch HANGARTNER/LOOSER, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 190 Rz. 11 mit Hinweisen auf Literatur und Rechtsprechung) und steht insbesondere einer verfassungskonformen Auslegung von Bundesgesetzen nicht entgegen (BGE 139 I 257 E. 4). Nach dem Wortlaut von Art. 190 BV sind Bundesgesetze und Völkerrecht gleichermassen massgebend. Im Konfliktfall geht das Völkerrecht jedoch grundsätzlich dem Bundesgesetzesrecht vor, insbesondere wenn die völkerrechtliche Norm – wie vorliegend die von den Beschwerdeführern angerufene EMRK – dem Schutz der Menschenrechte dient und keine völkerrechtskonforme Auslegung des anwendbaren Bundesgesetzesrechts möglich ist (BGE 139 I 16 E. 5.1 mit Hinweisen auf die Rechtsprechung; zum Verhältnis von Bundesgesetzesrecht und EMRK auch HANGARTNER/LOOSER, a.a.O., Art. 190 Rz. 38). Nach der Rechtsprechung des Bundesgerichts sind mithin Bundesgesetze auf ihre Vereinbar-

keit mit der EMRK hin zu überprüfen und es ist ihnen im Falle eines Widerspruchs grundsätzlich die Anwendbarkeit zu versagen (ASTRID EPINEY, in: Basler Kommentar zur BV, 2015, Art. 190 Rz. 40; KIENER/RÜTSCHE/KUHN, Öffentliches Verfahrensrecht, 2. Aufl. 2015, Rz. 1766).

Rechtsgrundlagen

7.

7.1 Die Beschwerdeführer verlangen, es seien die Anbieterinnen anzuweisen, gespeicherte Randdaten zu löschen und deren Speicherung zu unterlassen, soweit die Daten nicht für das Erbringen der vertraglichen Leistungen erforderlich seien. Zudem seien die Anbieterinnen zu verpflichten, dem Dienst oder einer anderen Behörde keine Daten herauszugeben. Zur Begründung machen sie im Wesentlichen geltend, die anlasslose Speicherung der Randdaten ihrer Telekommunikation verletze in schwerwiegender Weise ihren verfassungs- und völkerrechtlich geschützten Anspruch auf Achtung des Fernmeldeverkehrs sowie weitere Grundrechte. Der Grundrechtseingriff vermöge sich jedoch auf keine hinreichend bestimmte gesetzliche Grundlage zu stützen. Zudem liege die anlasslose Speicherung von Randdaten nicht im öffentlichen Interesse und sei insbesondere mit Blick auf verschiedene datenschutzrechtliche Grundsätze nicht verhältnismässig. Ihre Vorbringen begründen sie u.a. mit Verweisen auf die Rechtsprechung europäischer (Verfassungs-)Gerichte zur Speicherung von Randdaten und ein Urteil des Europäischen Gerichtshofs betreffend die europäische Richtlinie zur Vorratsdatenspeicherung (vgl. vorstehend Sachverhalt Bst. C.).

Zum Verständnis und zur Prüfung der Vorbringen der Beschwerdeführer im Zusammenhang mit der Verletzung ihrer Grundrechte ist es erforderlich, vorweg die gesetzliche (Verfahrens-)Ordnung betreffend die Speicherung – und Erhebung – von Randdaten des Fernmeldeverkehrs darzustellen (nachfolgend E. 7.2). Zudem ist auf die Bedeutung der aktuellen Totalrevision des BÜPF für die vorliegenden Beschwerdeverfahren einzugehen (nachfolgend E. 7.3).

7.2 Die Überwachung des Post- und Fernmeldeverkehrs fand sich zunächst umfassend im BÜPF geregelt. Mit Erlass der StPO wurden die strafprozessualen Bestimmungen im Wesentlichen in die StPO überführt (vgl. Art. 269 ff. StPO), während der eigentliche Vollzug der Überwachung des Post- und Fernmeldeverkehrs, also die technischen und organisatorischen Belange, weiterhin im BÜPF geregelt ist (Botschaft des Bundesrates vom

21. Dezember 2005 zur Vereinheitlichung des Strafprozessrechts, BBl 2006 1085, 1248). Das BÜPF legt im Wesentlichen die Pflichten der Anbieterinnen von Post- und Fernmeldedienstleistungen fest und regelt die Aufgaben der Vorinstanz (Art. 1 Abs. 2 und Art. 2 Abs. 1 sowie – betreffend die vorliegend interessierende Überwachung des Fernmeldeverkehrs – Art. 13 und Art. 15 BÜPF). Die Anbieterinnen sind demnach u.a. dazu verpflichtet, die Randdaten der Telekommunikation zu speichern, während sechs Monaten aufzubewahren und auf Verlangen hin der Vorinstanz zuzuleiten (Art. 15 Abs. 1 und 3 BÜPF). Der Dienst kann allerdings nur Auskünfte verlangen, wenn und soweit dies in einer Überwachungsanordnung der Staatsanwaltschaft festgehalten ist (Botschaft BÜPF, BBl 1998 IV 4241, 4279).

Die Staatsanwaltschaft kann unter bestimmten Voraussetzungen den Post- und Fernmeldeverkehr einer beschuldigten Person oder von Drittpersonen (inhaltlich) überwachen lassen (Art. 269 f. StPO). Die Anordnung einer Überwachung fällt in die ausschliessliche Zuständigkeit der Staatsanwaltschaft; dies gilt auch dann, wenn das Verfahren bei einem Gericht hängig ist (Urteil des BVGer A-5403/2011 vom 2. Mai 2012 E. 2). Neben der eigentlichen geheimen (inhaltlichen) Überwachung des Post- und Fernmeldeverkehrs kann die Staatsanwaltschaft Auskünfte einholen über die Randdaten der Telekommunikation, also etwa darüber, wann und mit welchen Personen eine überwachte Person über den Fernmeldeverkehr Verbindung gehabt hat (Art. 273 Abs. 1 StPO, vgl. zudem vorstehend E. 4.2). Voraussetzung einer entsprechenden Anordnung ist zunächst der dringende Verdacht, ein Verbrechen (Taten, die mit Freiheitsstrafe von mehr als drei Jahren bedroht sind [Art. 10 Abs. 2 des Schweizerischen Strafgesetzbuches [StGB, SR 311.0]) oder Vergehen (Taten, die mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bedroht sind [Art. 10 Abs. 3 StGB]) oder eine Übertretung nach Art. 179^{septies} StGB (Missbrauch einer Fernmeldeanlage) sei begangen worden (Art. 273 Abs. 1 StPO). Die Überwachungsmassnahme muss in einem direkten Sachzusammenhang zu dem untersuchten Delikt stehen (BGE 142 IV 34 E. 4.3.3). Darüber hinaus sind der Verhältnismässigkeits- bzw. der Subsidiaritätsgrundsatz zu beachten (Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 Bst. b und c StPO). Nach der Rechtsprechung genügt die voraussehbare Ineffizienz anderer Untersuchungsmassnahmen (JEAN-RICHARD-DIT-BRESSEL, a.a.O., Art. 269 Rz. 29 und 41–43; vgl. zudem Urteil des BGer 1B_265/2012 vom 21. August 2012 E. 2.3.1).

Die Anordnung einer (rückwirkenden) Überwachung wie der Erteilung von Auskunft über die Randdaten der Telekommunikation bedarf der (nachträglichen) Genehmigung durch das Zwangsmassnahmengericht (Art. 273 Abs. 2 StPO). Dieses entscheidet mit kurzer Begründung innert fünf Tagen seit der Anordnung der Überwachung oder der Auskunftserteilung und eröffnet den Entscheid unverzüglich der Staatsanwaltschaft sowie der Vorinstanz (Art. 274 [Abs. 2 und 3] StPO). Verweigert das Zwangsmassnahmengericht die Genehmigung, ist die Überwachung unverzüglich einzustellen (Art. 275 Abs. 1 Bst. b StPO). Dokumente und Datenträger aus einer nicht genehmigten Überwachung sind sofort zu vernichten und durch die Überwachung gewonnene Erkenntnisse dürfen nicht verwendet werden (Art. 277 StPO; vgl. auch HANSJAKOB, Kommentar StPO, Art. 277 Rz. 2 f.). Gegen (Nicht-)Genehmigungsentscheide des Zwangsmassnahmengerichts steht der Staatsanwaltschaft in Abweichung vom Grundsatz des doppelten Instanzenzuges die Beschwerde in Strafsachen an das Bundesgericht offen (BGE 137 IV 340 E. 2.1 und 2.2 mit Hinweisen; Urteil des BGer 1B_256/2015 vom 4. November 2015 E. 1 mit Hinweisen auf die Rechtsprechung; JEAN-RICHARD-DIT-BRESSEL, a.a.O., Art. 274 Rz. 10). Auskünfte über Randdaten können unabhängig von der Dauer der Überwachung und bis sechs Monate rückwirkend verlangt werden (Art. 273 Abs. 3 StPO, vgl. zudem Art. 15 Abs. 3 BÜPF; zum Ganzen auch BGE 142 IV 34 E. 4.1–4.3).

Die Anordnung der Staatsanwaltschaft ist bei der Vorinstanz einzureichen und hat – soweit sie die Überwachung des Fernmeldeverkehrs betrifft – die Angaben gemäss Art. 15 VÜPF bzw. Art. 23 VÜPF zu enthalten. Die Vorinstanz prüft, ob die Überwachung eine gemäss dem anwendbaren Recht überwachungsfähige Straftat betrifft und von der zuständigen Behörde angeordnet worden ist. Bei klar unrichtigen oder unbegründeten Anordnungen nimmt sie mit der Genehmigungsbehörde – dem Zwangsmassnahmengericht – Kontakt auf, bevor sie Informationen an die anordnende Behörde weiterleitet (Art. 13 Abs. 1 Bst. a BÜPF). Die Überprüfungsbefugnis der Vorinstanz ist somit – auch nach den Materialien – auf eine formelle Prüfung der Überwachungsanordnung beschränkt (Botschaft BÜPF, BBl 1998 IV 4241, 4277); eine weitergehende Prüfung ist nicht möglich, da die Vorinstanz keine Übersicht über die strafprozessuale Untersuchung und sich auch nicht damit zu befassen hat (vgl. zum Ganzen auch HANSJAKOB, Kommentar BÜPF / VÜPF, Art. 13 BÜPF Rz. 3 und 4 unter Verweis auf die Kommentierung zu Art. 11 Abs. 1 Bst. a und b BÜPF; vgl. auch nachfolgend E. 8.2). Die Vorinstanz weist die Anbieterinnen sodann an, die für die Überwachung notwendigen Massnahmen zu treffen (Art. 13 Abs. 1 Bst. b

BÜPF). Diese beschränken sich auf die technischen und organisatorischen Anweisungen über die durchzuführenden Massnahmen; die Anbieterinnen sollen nicht erfahren, ob die überwachte Person verdächtig ist oder als Drittperson überwacht wird und welche Straftaten verfolgt werden (Botschaft BÜPF, BBl 1998 IV 4241, 4279). Die Anbieterinnen liefern der Vorinstanz die verlangten Randdaten so rasch als möglich (Art. 15 Abs. 1 und 4 BÜPF). Diese nimmt die Randdaten des Fernmeldeverkehrs entgegen und leitet sie an die anordnende Behörde weiter (Art. 13 Abs. 1 Bst. e BÜPF). Die Vorinstanz betreibt zu diesem Zweck ein Verarbeitungszentrum. Dort werden die Randdaten bereitgestellt und können von der zuständigen Strafverfolgungsbehörde online abgerufen werden (Art. 8 Abs. 1–3 VÜPF). Die Vorinstanz kann der anordnenden Strafverfolgungsbehörde die Randdaten auch in Form von Datenträgern und Dokumenten durch Versand auf dem Postweg übermitteln (Art. 8 Abs. 4 VÜPF; vgl. auch HANSJAKOB, Kommentar BÜPF / VÜPF, Art. 13 BÜPF Rz. 11; Botschaft nBÜPF, BBl 2013 2683, 2728).

Die Überwachung des Fernmeldeverkehrs ist grundsätzlich geheim (Art. 279 StPO, Art. 17 Abs. 7 und Art. 25 Abs. 7 VÜPF). Dies gilt auch für Auskünfte über Randdaten i.S.v. Art. 273 StPO (vgl. Urteil des BGer 1B_251/2013 vom 30. August 2013 E. 4.2). Die Staatsanwaltschaft teilt der überwachten beschuldigten Person und den nach Art. 270 Bst. b StPO überwachten Drittpersonen spätestens mit Abschluss des Vorverfahrens Grund, Art und Dauer der Überwachung mit (Art. 279 Abs. 1 StPO). Erforderlich ist eine förmliche Mitteilung (Urteil des BGer 6B_582/2013 vom 20. Februar 2014 E. 2.3 und E. 2.4.2). Die Mitteilung kann mit Zustimmung des Zwangsmassnahmengerichts aufgeschoben oder unterlassen werden, wenn die Erkenntnisse nicht zu Beweiszwecken verwendet werden bzw. wenn der Aufschub oder das Unterlassen zum Schutze überwiegender öffentlicher oder privater Interessen notwendig ist (Art. 279 Abs. 2 StPO). Betroffene können nachträglich, d.h. nach erfolgter Mitteilung, die Überwachung auf dem Beschwerdeweg anfechten (Art. 279 Abs. 3 StPO; vgl. auch Urteil des BGer 6B_582/2013 vom 20. Februar 2013 E. 2.3; zur Anfechtbarkeit des Beschwerdeentscheids vor Bundesgericht bzw. zum Erfordernis eines nicht wieder gutzumachenden Nachteils vgl. Urteil des BGer 6B_57/2015 vom 27. Januar 2016 E. 3.2.1 mit Hinweisen auf die Rechtsprechung).

Totalrevision des BÜPF

7.3

7.3.1 Das BÜPF wurde einer Totalrevision unterzogen. Der Entwurf wurde am 18. März 2016 vom Gesetzgeber angenommen. Die Referendumsfrist lief am 7. Juli 2016 unbenutzt ab (BBl 2016 1991). Es fragt sich daher, ob und gegebenenfalls in welcher Form die Totalrevision des BÜPF für das vorliegende Beschwerdeverfahren zu berücksichtigen ist. Darauf ist im Folgenden einzugehen.

7.3.2 Inwieweit Rechtsänderungen, die erst nach Erlass einer angefochtenen Verfügung eingetreten sind, zu berücksichtigen sind, hängt von der massgeblichen gesetzlichen Übergangsbestimmung ab. Fehlt eine solche, ist gestützt auf die allgemeinen übergangsrechtlichen Grundsätze zu entscheiden. Nach der Rechtsprechung bleibt grundsätzlich diejenige Regelung anwendbar, welche im Zeitpunkt des Eintritts des Sachverhalts, den es rechtlich zu beurteilen gilt oder der zu Rechtsfolgen führt, in Kraft stand (BGE 136 V 24 E. 4.3; Urteil des BGer 8C_263/2011 vom 31. Oktober 2011 E. 8.1). Nachher eingetretene Rechtsänderungen haben grundsätzlich unberücksichtigt zu bleiben, insbesondere wenn sich der massgebende Sachverhalt abschliessend vor Inkrafttreten des geänderten Rechts verwirklich hat (Verbot der echten Rückwirkung; Urteil des BGer 2C_477/2013 vom 16. Dezember 2013 E. 2.4 mit Hinweisen auf die Rechtsprechung; Urteil des BVGer A-2849/2014 vom 28. Oktober 2014 E. 5.2.2; zum Ganzen zudem HÄFELIN/MÜLLER/UHLMANN, Allgemeines Verwaltungsrecht, 7. Aufl. 2016, Rz. 268 f., 288–292).

Eine Ausnahme vom Verbot der echten Rückwirkung ist dann zu machen, wenn zwingende Gründe dafür bestehen, das neue Recht sogleich anzuwenden. Entsprechendes hat das Bundesgericht etwa bei Bestimmungen im Bereich des Umweltschutzes erkannt (BGE 139 II 470 E. 4.2 mit Hinweisen; Urteil des BGer 1C_23/2014, 1C_25/2014 vom 24. März 2015 E. 7.4.2 f.). Selbst in einem solchen Fall findet die Anwendung des neuen Rechts jedoch eine Grenze im Grundsatz von Treu und Glauben (vgl. HÄFELIN/MÜLLER/UHLMANN, a.a.O., Rz. 295). Ferner ist bei offenen, im Zeitpunkt der Rechtsänderung noch andauernden Sachverhalten in der Regel das neue (materielle) Recht anzuwenden, sofern die Anwendung neuen Rechts nicht mit dem Vertrauensschutz kollidiert, welcher u.U. einen Anspruch auf eine angemessene Übergangsregelung begründet (sog. unechte Rückwirkung; MOSER/BEUSCH/KNEUBÜHLER, Prozessieren vor dem

Bundesverwaltungsgericht, 2. Aufl. 2013, Rz. 2.203 mit Hinweisen auf die Rechtsprechung).

Unzulässig ist auf der anderen Seite die Anwendung von noch nicht in Kraft gesetzten Rechts unter Nichtanwendung des geltenden Rechts (sog. positive Vorwirkung; BGE 136 I 142 E. 3.2). Dies gilt selbst dann, wenn der Gesetzgeber eine Revision der anwendbaren Bestimmungen beschlossen hat (Urteil des BGer 1C_179/2013 vom 15. August 2013 E. 3.7 mit Hinweisen auf die Rechtsprechung). In beschränktem Masse zulässig ist die negative Vorwirkung zukünftigen Rechts. Eine solche liegt vor, wenn das geltende Recht bis zum Inkrafttreten neuen Rechts nicht mehr angewendet wird. Dies ist nur zulässig, wenn das geltende Recht Entsprechendes vorsieht (vgl. hierzu BGE 136 I 142 E. 3.2 sowie HÄFELIN/MÜLLER/UHLMANN, a.a.O., Rz. 302 f.).

7.3.3 Der Bundesgesetzgeber beschloss am 18. März 2016 eine Totalrevision des BÜPF. Das totalrevidierte BÜPF ist jedoch noch nicht in Kraft, weshalb sich die Frage einer allfälligen Rückwirkung des neuen Rechts auf die vorliegend zu beurteilenden Sachverhalte nicht stellt. Es ist einzig zu prüfen, ob dem totalrevidierten BÜPF im vorliegenden Beschwerdeverfahren bzw. auf die vorliegend zu beurteilende Streitsache ausnahmsweise eine Vorwirkung zukommt. Dies ist zu verneinen. Eine positive Vorwirkung nicht in Kraft gesetzten Rechts – vorliegend des totalrevidierten BÜPF – ist wie vorstehend dargestellt nicht zulässig. Zudem besteht keine gesetzliche Bestimmung, welche die Anwendung des geltenden BÜPF bis zum Inkrafttreten des geänderten Rechts untersagen würde, was auch eine negative Vorwirkung ausschliesst. Die angefochtenen negativen Verfügungen sind daher gestützt auf das geltende Recht zu beurteilen.

Nach der Rechtsprechung ist es jedoch zulässig, dass die Materialien zum totalrevidierten BÜPF bei der Auslegung einer Norm des geltenden Rechts im Sinne einer geltungszeitlichen Auslegung berücksichtigt werden. Dies gilt namentlich dann, wenn das geltende System nicht grundsätzlich geändert werden soll, sondern nur eine Konkretisierung des bestehenden Rechtszustandes angestrebt wird oder (echte) Lücken des geltenden Rechts ausgefüllt werden sollen (BGE 141 II 297 E. 5.5.3; BGE 131 II 13 E. 7.1; Urteil des BGer 2C_386/2014 vom 18. Januar 2016 E. 7.5; vgl. auch BGE 139 IV 195 E. 2.3). Zudem ist nicht von vornherein ausgeschlossen, die vom Gesetzgeber im Zusammenhang mit der Totalrevision des BÜPF vorgenommenen Wertungen im Rahmen der Prüfung der Verhältnismässigkeit eines allfälligen Grundrechtseingriffs zu berücksichtigen. So hielt

das Bundesgericht in einem Urteil vom 15. März 2012 fest, eine neue, noch nicht in Kraft gesetzte Regelung im Raumplanungsgesetz (RPG, SR 700) sei geeignet, sich auf die (materielle) Beurteilung der im Streit liegenden Sache – zu beurteilen war der Abbruch eines ohne Baubewilligung erstellten Wohnhauses – auszuwirken. Aus diesem Grund sei es i.S.v. Art. 36 BV unverhältnismässig, den Abbruch des Wohnhauses zu verfügen, ohne die Möglichkeit der Anwendung der neuen Bestimmung eingehender zu prüfen. Daran ändere nichts, dass die Neuregelung des Gesetzes noch nicht in Kraft sei (Urteil des BGer 1C_187/2011 vom 15. März 2012 E. 3; ALAIN GRIFFEL, Intertemporales Recht aus dem Blickwinkel des Verwaltungsrechts, in: Uhlmann [Hrsg.], Intertemporales Recht aus dem Blickwinkel der Rechtsetzungslehre und des Verwaltungsrechts, 13. Jahrestagung des Zentrums für Rechtsetzungslehre, 2014, S. 20 f.). Für eine entsprechende Berücksichtigung des totalrevidierten BÜPF im vorliegenden Beschwerdeverfahren ist nach der zitierten Erwägungen des Bundesgerichts somit (implizit) vorausgesetzt, dass – wie geschehen – gegen die Totalrevision des BÜPF nicht das Referendum ergriffen wird oder diese in einer Volksabstimmung angenommen worden ist und somit (in Kürze) mit dem Inkrafttreten des totalrevidierten BÜPF gerechnet werden kann.

7.4 Vor diesem Hintergrund sind im Folgenden die Vorbringen der Beschwerdeführer zu prüfen, wobei zunächst zu beurteilen ist, ob die Vorinstanz auf die Rechtsbegehren der Beschwerdeführer zu Recht teilweise nicht eingetreten ist.

Herausgabe von Randdaten an andere Behörden und Gerichte

8.

8.1 Die Beschwerdeführer hatten von der Vorinstanz verlangt, die Anbieterinnen anzuweisen, keine Randdaten i.S.v. Art. 15 Abs. 3 BÜPF an die Vorinstanz oder an andere Behörden oder an Gerichte herauszugeben (Antrag Ziff. 2: vgl. vorstehend Sachverhalt Bst. A). Die Vorinstanz trat darauf nicht ein. Sie erwog sinngemäss, Randdaten dürften nur gestützt auf eine (genehmigte) Überwachungsanordnung erhoben werden, welche gemäss Art. 279 Abs. 3 StPO nachträglich mit Beschwerde angefochten werden könnte. Es fehle daher – mangels Vorliegens von Überwachungsanordnungen – an einem hinreichend aktuellen schutzwürdigen Interesse, über den betreffenden Antrag der Beschwerdeführer verfügungsweise zu entscheiden.

8.2 Das geltende Recht zur Überwachung des Post- und Fernmeldeverkehrs sieht – wie vorstehend erwogen – eine Trennung von verwaltungsrechtlichen und strafprozessualen Aspekten vor. Das BÜPF und die StPO haben unterschiedliche Adressaten und verfolgen unterschiedliche Regelungszwecke. Während die StPO die Strafverfolgung und Beurteilung der Straftaten nach Bundesrecht durch die Strafbehörden des Bundes und der Kantone regelt (Art. 1 Abs. 1 StPO) und die beschuldigte Person im Fokus steht, stellt das BÜPF die technische und organisatorische Umsetzung einer strafprozessual zulässigen Überwachung sicher. Das verwaltungsrechtliche Verfahren steht in diesem Sinne neben dem strafprozessualen. Das BÜPF richtet sich an die Anbieterinnen von Fernmeldedienstleistungen und regelt die Aufgaben der Vorinstanz. Es bestimmt, wie die Anbieterinnen bei einer solchen Überwachung zur Mitwirkung verpflichtet werden können, während sich die gesetzliche Grundlage für die Überwachung selbst in der StPO findet (vgl. vorstehend E. 7.2; zudem BGE 139 IV 195 E. 2.2).

Entsprechend der Trennung der verwaltungsrechtlichen von den strafprozessualen Aspekten der Überwachung unterscheiden sich auch die sachliche Zuständigkeit und Überprüfungsbefugnis von Staatsanwaltschaft bzw. Genehmigungsbehörde und der Vorinstanz. Die Staatsanwaltschaft ordnet die Überwachung an, wenn die strafprozessualen Voraussetzungen von Art. 269 ff. StPO gegeben sind. Diese wird von der Genehmigungsbehörde (nachträglich) überprüft. Der beschuldigten Person steht gegen die Überwachungsanordnung – nach erfolgter Mitteilung der Überwachung durch die Staatsanwaltschaft – die Beschwerde nach den Art. 393–397 StPO offen (Art. 279 Abs. 3 StPO). Die Vorinstanz prüft alsdann in strafprozessualer Hinsicht lediglich noch formell, ob die Überwachung eine gemäss dem anwendbaren Recht überwachungsfähige Straftat betrifft und von der zuständigen Behörde angeordnet worden ist (Art. 13 Abs. 1 Bst. a BÜPF; Botschaft BÜPF, BBl 1998 IV 4241, 4277); die Frage, ob die Voraussetzungen für eine Überwachung gegeben sind und ob eine konkrete Überwachungsanordnung verhältnismässig ist, ist einzig von der Staatsanwaltschaft und der Genehmigungsbehörde zu beurteilen und kann nach erfolgter Mitteilung auf Beschwerde hin gerichtlich überprüft werden (Urteil des BGer 1A.188/2003 vom 13. April 2004, E. 2.2.2; BVGE 2009/46 E. 3.1 und 8.3).

Die materielle Überprüfungsbefugnis der Vorinstanz beschränkt sich auf die verwaltungsrechtlichen Aspekte der Überwachung. Sie hat im Hinblick auf die technische und organisatorische Umsetzung der Überwachung

durch die Anbieterinnen etwa zu prüfen, ob sich eine Überwachungsmassnahme auf eine hinreichende gesetzliche Grundlage im BÜPF stützt, wenn eine Anbieterin geltend macht, eine bestimmte Art der Überwachung fordere von ihr Kenntnisse und technische Mittel, über die sie nicht verfüge (BVGE 2009/46 E. 3-8; Urteil des BVGer A-8284/2010 vom 21. Juni 2011 E. 3; vgl. zudem einschränkender BGE 130 II 249 E. 2.2.2 f.). Gegen Verfügungen der Vorinstanz steht (den Anbieterinnen bzw. den Mitwirkungspflichtigen) der Weg der Verwaltungsrechtspflege offen (Art. 32 VÜPF; hierzu auch HANSJAKOB, Kommentar BÜPF / VÜPF, Art. 32 VÜPF Rz. 2 f. und 5; vgl. auch die Botschaft nBÜPF, BBl 2013 2683, 2764–2766, worin der Bundesrat unter Verweis auf die bisherige Rechtsprechung und die Lehre die Dualität des Rechtsschutzes betont und ausführt, dass im Rahmen der Verwaltungsrechtspflege die Überprüfung strafprozessualer Aspekte ausgeschlossen ist). Wie weit diese Überprüfungsbefugnis der Vorinstanz – und hiernach des Bundesverwaltungsgerichts – im Einzelfall geht und welches die Reflexwirkungen auf die strafprozessuale Anordnung sind, kann vorliegend offen bleiben. Immerhin ist festzuhalten, dass der Wortlaut von Art. 13 Abs. 1 Bst. a BÜPF, welcher die Überprüfungsbefugnis der Vorinstanz bezüglich der strafprozessualen Aspekte regelt und einschränkt, eine (umfassende) Überprüfungsbefugnis in verwaltungsrechtlicher Hinsicht nicht von vornherein ausschliesst (vgl. kritisch auch zur Rechtsprechung HEINIGER, a.a.O., insbes. Rz. 3 ff. und 26 ff.; betreffend die mit der Totalrevision in diesem Zusammenhang geplanten Neuerungen bzw. Präzisierungen Botschaft nBÜPF, BBl 2013 2683, 2723–2725).

8.3 Nach den Rechtsbegehren der Beschwerdeführer sind die Anbieterinnen anzuweisen, keine Randdaten an die Vorinstanz oder an andere Behörden oder an Gericht herauszugeben. Abgesehen davon, dass diesbezüglich vorliegend ohnehin einzig das Nichteintreten der Vorinstanz zu beurteilen ist (vgl. vorstehend E. 4.3), ist vorab festzuhalten, dass eine Herausgabe von Randdaten durch die Anbieterinnen *direkt* an andere Behörden oder an Gerichte gesetzlich nicht vorgesehen ist; die Anbieterinnen sind nach Art. 15 Abs. 1 BÜPF verpflichtet, der Vorinstanz auf Verlangen und gestützt auf eine Überwachungsanordnung der zuständigen Behörde die Randdaten zuzuleiten (vgl. hierzu sogleich E. 8.4). Soweit die Rechtsbegehren der Beschwerdeführer in der Sache eine Herausgabe von Randdaten an andere Behörde oder an Gericht betreffen, ist somit darauf nicht näher einzugehen. Soweit die Herausgabe von Randdaten an die Vorinstanz betroffen ist, ist im Folgenden zu prüfen, ob die Vorinstanz auf die Anträge der Beschwerdeführer zu Recht nicht eingetreten ist.

8.4 Die Vorinstanz kann von den Anbieterinnen das Zuleiten von Randdaten nur verlangen, wenn und soweit dies in einer (genehmigten) Überwachungsanordnung festgehalten ist (Botschaft BÜPF, BBl 1998 IV 4241, 4279). Hiergegen steht der beschuldigten Person nachträglich die Beschwerde gemäss Art. 393–397 StPO offen (Art. 297 Abs. 3 StPO). Die Frage, ob gespeicherte Randdaten gestützt auf eine Überwachungsanordnung herausgegeben werden dürfen, ist mithin zunächst von der Genehmigungsbehörde und – nach erfolgter Mitteilung an die beschuldigte Person – allenfalls von der Beschwerdeinstanz zu beurteilen. In diesem Verfahren ist die rechtsstaatliche Absicherung der Grundrechte gewährleistet (vgl. in diesem Sinn gestützt auf die bisherige Rechtsprechung die Botschaft nBÜPF, BBl 2013 2683, 2748). Das Zuleiten von gespeicherten Randdaten betrifft demnach die strafprozessualen Aspekte der Überwachung des Fernmeldeverkehrs. Aus diesem Grund ist und war die Vorinstanz zum Entscheid über Antrag Ziff. 2 der Beschwerdeführer sachlich nicht zuständig und ist somit mangels Vorliegens einer erforderlichen Sachentscheidvoraussetzung auf die betreffenden Anträge zu Recht nicht eingetreten. Daran ändert – für sich alleine – nichts, dass der beschuldigten Person im Rahmen einer konkreten Überwachung erst nachträglich die Möglichkeit geboten ist, Beschwerde gegen eine Überwachungsanordnung zu erheben (BGE 130 II 249 E. 2.2.3).

Bei diesem Ergebnis erübrigt es sich, auf die Frage einzugehen, ob die Beschwerdeführer an einem Entscheid in der Sache ein aktuelles und schutzwürdiges Interesse besitzen, was von der Vorinstanz verneint wird. Die Beschwerden sind abzuweisen, soweit die Beschwerdeführer sinngemäss beantragt haben, es sei die Vorinstanz zu verpflichten, über ihren Antrag Ziff. 2 materiell zu entscheiden.

8.5 Hinzuweisen ist in diesem Zusammenhang schliesslich auf das Folgende: Die Beschwerdeführer stellen verschiedentlich die Vereinbarkeit der strafprozessualen Ordnung für die (nachträgliche) Überwachung des Post- und Fernmeldeverkehrs mit ihren Grundrechten in Frage. Sie kritisieren insbesondere, die Voraussetzungen für die Anordnung einer Überwachung und der Gegenstand der Überwachung seien im Gesetz nicht hinreichend bestimmt bzw. eng umschrieben und die erst nachträglich erforderliche Genehmigung durch das Zwangsmassnahmengericht erlaube die sofortige Verwendung von Randdaten. Die Folge ist nach Ansicht der Beschwerdeführer ein unzureichender Schutz vor ungerechtfertigten Überwachungsmassnahmen. Zudem würden, obschon in Art. 197 Abs. 1 Bst. b

StPO verlangt, Randdaten etwa im Rahmen einer Rasterfahndung und damit im Rahmen einer Zwangsmassnahme auch dann verwendet, wenn (noch) kein hinreichender Tatverdacht vorliege.

Diese Vorbringen, welche sich an die Erwägungen des Europäischen Gerichtshofes in dessen Urteil vom 8. April 2014 anlehnen (vgl. vorstehend Sachverhalt Bst. C), betreffen – wie vorstehend ausgeführt – die strafprozessualen Aspekte der Überwachung und gehen damit über das hinaus, was die Vorinstanz im Rahmen ihrer sachlichen Zuständigkeit zu verfügen befugt ist und somit auch vom Bundesverwaltungsgericht in diesem Verfahren nicht überprüft werden kann. Darüber hinaus ist es dem Bundesverwaltungsgericht verwehrt, die Bestimmungen eines Bundesgesetzes – wie z.B. der StPO – abstrakt auf ihre Vereinbarkeit mit grundrechtlich geschützten Positionen hin zu überprüfen. Die abstrakte Normenkontrolle, d.h. die Überprüfung der Gültigkeit einer Norm bzw. eines Erlasses abstrakt in einem besonderen Verfahren und somit unabhängig von einer konkreten Anwendung, ist auf Bundesebene auf die Überprüfung kantonaler Erlasse im Rahmen der Beschwerde in öffentlich-rechtlichen Angelegenheiten an das Bundesgericht beschränkt (Art. 82 Bst. b des Bundesgerichtsgesetzes [BGG, SR 173.110]; KIENER/RÜTSCHE/KUHN, Öffentliches Verfahrensrecht, 2. Aufl. 2015, Rz. 1712). Dagegen beurteilt das Bundesverwaltungsgericht Beschwerden gegen Verfügungen nach Art. 5 VwVG, welche sich auf einen individuell-konkreten Sachverhalt beziehen (Art. 31 VGG). Eine abstrakte Überprüfung von strafprozessualen Bestimmungen auf ihre Vereinbarkeit mit den Grundrechten und völkerrechtlichen Garantien ist daher im vorliegenden Verfahren von vornherein nicht möglich und die Beschwerdeführer mit ihren diesbezüglichen Vorbringen aus diesem Grund nicht zu hören (zur Herausgabe bzw. Bekanntgabe von Randdaten an die Strafverfolgungsbehörden aus Sicht des Grundrechtsschutzes vgl. BGE 139 IV 98 E. 4 und BGE 126 I 50 E. 6, insbes. E. 6b).

Grundrechtseinschränkung

9.

9.1 Im Folgenden ist zu beurteilen, ob die Vorinstanz den Antrag der Beschwerdeführer, es seien die Anbieterinnen anzuweisen, gespeicherte Randdaten zu löschen und deren Speicherung zu unterlassen, soweit die Daten nicht für die Erbringung der vertraglichen Leistungen erforderlich seien (Antrag Ziff. 1; vorliegend Antrag Ziff. 2), zu Recht abgewiesen hat.

Die Speicherung von Randdaten verletzt nach Ansicht der Beschwerdeführer in schwerwiegender Weise ihren grund- und völkerrechtlich geschützten Anspruch auf Achtung des Fernmeldeverkehrs bzw. das Fernmeldegeheimnis und auf Schutz vor Missbrauch ihrer persönlichen Daten. Zudem würden ihre ebenfalls grund- und völkerrechtlich geschützte persönliche Freiheit, ihre Meinungs-, Medien- und Versammlungsfreiheit sowie die Garantie der Unschuldsvermutung eingeschränkt. Das Fernmeldegeheimnis verleihe jeder Person das Recht, frei von staatlicher Überwachung mit anderen Personen zu kommunizieren. Geschützt seien sowohl der Inhalt der Kommunikation als auch die Tatsache an sich, dass eine Kommunikation stattfindet und deren äusseren Umstände wie Ort und Zeit des Kommunikationsvorgangs sowie die Identität der daran teilnehmenden Personen. Die Beschwerdeführer halten sinngemäss dafür, die Speicherung von Randdaten bewirke ein subjektives Gefühl des Überwachtwerdens, so dass bereits die blosse Möglichkeit einer (rückwirkenden) Überwachung einen Eingriff in das Fernmeldegeheimnis sowie die Meinungs- und die Medienfreiheit darstelle. Hierfür fehlt es nach Ansicht der Beschwerdeführer an einer hinreichend bestimmten gesetzlichen Grundlage und an einem überwiegenden öffentlichen Interesse. Betroffene könnten anhand der gesetzlichen Bestimmungen nicht ermessen, welche Daten zu welchem Zweck gespeichert würden und der Nutzen für die Strafverfolgung stehe angesichts der Verletzung verschiedener datenschutzrechtlicher Grundsätze in einem Missverhältnis zu der damit verbundenen Grundrechtseinschränkung.

Es ist somit zu prüfen, welche Garantien das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung, auf welche sich die Beschwerdeführer in erster Linie berufen, enthalten, welche Formen von Einschränkungen sie zulassen und welche Anforderungen sie an die streitbetroffene Speicherung und Aufbewahrung von Randdaten der Telekommunikation stellen (nachfolgend E. 9.2 ff.). Zu untersuchen sind alsdann das Vorliegen einer gesetzlichen Eingriffsgrundlage, deren Qualität hinsichtlich Bestimmtheit und Voraussehbarkeit (nachfolgend E. 10), die öffentlichen Interessen an der Speicherung und Aufbewahrung der Randdaten (nachfolgend E. 11) sowie die Verhältnismässigkeit der allfälligen Einschränkung geschützter Grundrechtspositionen einschliesslich des Vorhandenseins von Kontrollmechanismen (nachfolgend E. 12; Art. 36 BV).

9.2

9.2.1 Nach Art. 13 Abs. 1 BV hat jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und

Fernmeldeverkehrs (Fernmeldegeheimnis). Gleichartige Garantien ergeben sich aus Art. 8 Ziff. 1 EMRK und Art. 17 des Internationalen Paktes vom 16. Dezember 1966 über bürgerliche und politische Rechte (UNO-Pakt II, SR 0.103.2; für die Schweiz in Kraft seit 18. September 1992; BGE 140 I 353 E. 8.3; BGE 109 Ia 273 E. 4a; STEPHAN BREITENMOSER, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 13 Rz. 2; zum Schutzbereich von Art. 8 EMRK GRABENWARTER/PABEL, Europäische Menschenrechtskonvention, 6. Aufl. 2016, § 22 Rz. 5–25). Zudem hat nach Art. 13 Abs. 2 BV jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Die Verfassungsbestimmung von Art. 13 BV schützt – wie Art. 8 EMRK – die Privatsphäre als Raum für die Entwicklung und Entfaltung der individuellen Persönlichkeit. Sie steht allen (natürlichen) Personen zu (KIENER/KÄLIN, Grundrechte, 2. Aufl. 2013, S. 166). Geschützt sind die Identität, die sozialen Beziehungen und das private Verhalten jeder natürlichen Person, die Ehre und der Ruf sowie namentlich alle sich auf Personen beziehende Informationen, die nicht allgemein zugänglich sind (BGE 140 I 381 E. 4.1). Eingeschlossen ist auch die (mit fremden Mitteln geführte) individuelle private und geschäftliche Kommunikation gegenüber Drittpersonen (BERANEK ZANON/DE LA CRUZ BÖHRINGER, in: Passadelis/Rosenthal/Thür [Hrsg.], Datenschutzrecht, 2015, § 9 Rz. 9.23; Urteil des EGMR Copland gegen Vereinigtes Königreich vom 3. April 2007, 62617/00, § 41). Diese soll vertraulich und geheim geführt werden können, ohne dass das Gemeinwesen Einblick erhält und daraus gewonnene Erkenntnisse gegen den Betroffenen verwendet. Betroffene dürfen mit der Vertraulichkeit der Kommunikation rechnen. Auf diese ist der Schutz von Art. 13 Abs. 1 BV und unter dem Begriff der Korrespondenz der Schutz von Art. 8 Ziff. 1 EMRK ausgerichtet; sie bildet den Schutzweck des Fernmeldegeheimnisses (MÜLLER/SCHEFER, a.a.O., S. 205; STÉPHANE BONDALLAZ, La protection des personnes et de leurs données dans les télécommunications, 2007, Rz. 1062 und 1113; Urteil des EGMR Michaud gegen Frankreich vom 6. Dezember 2012, 12323/11, § 90).

Auszugehen ist von der Achtung des umfassend zu verstehenden Fernmeldeverkehrs, unbesehen der Art der fernmeldetechnischen Übertragung. Der sachliche Schutzbereich bezieht sich somit nicht nur auf den Inhalt der Kommunikation, sondern schliesst grundsätzlich auch die Randdaten als integralen Bestandteil der Telefongespräche ein. Geschützt ist mithin auch die Tatsache, dass überhaupt zwischen zwei Fernmeldeteilnehmern ein individueller Informationsaustausch stattgefunden hat (BGE

140 I 353 E. 8.3 mit Hinweisen auf die Rechtsprechung und Literatur; Urteil des EGMR Malone gegen Vereinigtes Königreich vom 2. August 1984, 8691/79, § 84; OLIVER DIGGELMANN, in: Basler Kommentar zur BV, 2015; Art. 13 Rz. 29; MÜLLER/SCHEFER, a.a.O., S. 203–205; KATIA FAVRE, Sorgfaltspflichten bei der Datenübertragung, 2006, S. 81–83; ROLF H. WEBER, Fernmeldegeheimnis und Datenschutz, in: Weber [Hrsg.], Neues Fernmelderecht, 1998, S. 189, nachfolgend: Fernmeldegeheimnis). Der Schutzbereich des Fernmeldegeheimnisses greift jedoch nicht beliebig weit, sondern ist in sachlicher Hinsicht auf den Kommunikationsvorgang beschränkt; vor dessen Beginn und nach dessen Abschluss greift das Fernmeldegeheimnis nicht (BGE 140 IV 181 E. 2, insbes. E. 2.3 f.).

Als besonderen Teilaspekt des Rechts auf Privatsphäre gewährt Art. 13 Abs. 2 BV einen Anspruch auf Schutz vor Missbrauch persönlicher Daten (GIOVANNI BIAGGINI, Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft, 2007, Art. 13 Rz. 11). Dieser Wortlaut ist nach der Rechtsprechung zu eng. Der sachliche Schutzbereich erfasst nicht nur den Missbrauch, sondern – im Kontext und mit Blick auf die Autonomie des Einzelnen hinsichtlich der Entfaltung seiner Persönlichkeit – grundsätzlich jeden Umgang des Staates mit persönlichen Daten bzw. jede staatliche Bearbeitung wie das Erheben, Sammeln, Aufbewahren, Speichern sowie die Weiter- und Bekanntgabe (Recht auf informationelle Selbstbestimmung; BGE 128 II 259 E. 3.2; Urteil des BGer 1C_74/2015 vom 2. Dezember 2015 E. 4.1; Urteil des BGer 6B_4/2011 vom 28. November 2011 E. 2.3 f.; vgl. auch BGE 138 II 346 E. 8.2; BGE 122 I 360 E. 5a; RAINER J. SCHWEIZER, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 13 Rz. 74; BELSER, a.a.O., § 6 Rz. 58–61, 86–89 sowie 96; MÜLLER/SCHEFER, a.a.O., S. 170; ROLF H. WEBER, Grundrecht auf Vertraulichkeit und Integrität, digma 2008, S. 55–58). Denselben Schutz bietet grundsätzlich auch Art. 8 Ziff. 1 EMRK (BGE 138 I 256 E. 4; BGE 138 I 6 E. 4.1 mit Hinweisen auf die Rechtsprechung des EGMR, insbesondere auf das Urteil des EGMR Amann gegen die Schweiz vom 16. Februar 2000, 27798/95, § 65 und 69; GRABENWARTER/PABEL, a.a.O., § 22 Rz. 10 f.).

Als persönliche Daten gelten – entsprechend der Definition in Art. 3 Bst. a DSG – alle Angaben, die einen hinreichend engen Bezug zu einer bestimmten oder bestimmbaren Person aufweisen (BELSER, a.a.O., § 6 Rz. 90). Der sachliche Schutzbereich ist im Einzelfall anhand des Schutzziels von Art. 13 Abs. 2 BV zu bestimmen; das Recht auf informationelle Selbstbestimmung schützt dabei als Teilaspekt der Privatsphäre die Person und nicht die Daten (SIGRIST, a.a.O., S. 38). Der Anspruch auf Schutz

vor Missbrauch persönlicher Daten begründet in erster Linie Abwehransprüche des Einzelnen. Dieser soll selbst bestimmen dürfen, wer welches Wissen über ihn haben darf bzw. welche personenbezogenen Begebenheiten und Ereignisse des konkreten Lebens dem Staat oder einer weiteren Öffentlichkeit verborgen bleiben sollen (vgl. BGE 138 II 346 E. 8.2). Teils werden jedoch auch Ansprüche auf staatliches Tätigwerden und darüber hinaus den Gesetzgeber ansprechende Schutzpflichten angenommen, welchen dieser etwa mit Erlass des DSG nachgekommen ist (vgl. Art. 1 DSG; Urteil des BGer 2C_1065/2014 vom 26. Mai 2016 E. 6.1 [zur Publikation vorgesehen]; BGE 137 I 167 E. 3.2 mit Hinweisen; BGE 122 I 360 E. 5b/dd; SIGRIST, a.a.O., S. 19; zu den Ansprüchen aus Art. 13 Abs. 2 BV vgl. BELSER, a.a.O., § 6 Rz. 97 ff.; zur Umsetzung der Schutzpflichten BELSER, a.a.O., § 6 Rz. 111 und MÜLLER/SCHEFER, a.a.O., S. 174).

9.2.2 Der EGMR bezeichnet den Begriff des Privatlebens i.S.v. Art. 8 EMRK als einen weiten Begriff, der einer abschliessenden Umschreibung nicht zugänglich ist. Es umfasst physische und psychische Aspekte und räumt dem Einzelnen einen Anspruch auf persönliche Identität und Entfaltung ein. Zum Privatleben gehört, dass ungehindert Beziehungen mit anderen Personen geknüpft und gepflegt werden können (Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010, 35623/05, § 43). In diesem Sinne schützt Art. 8 EMRK die Vertraulichkeit der Kommunikation (vgl. Urteil des EGMR Michaud gegen Frankreich vom 6. Dezember 2012, 12323/11, § 90). Ebenfalls in den Schutzbereich von Art. 8 EMRK fallen persönliche Daten bzw. die Privatsphäre betreffende Daten. Dies schliesst einen Schutz vor staatlicher Erhebung, Speicherung, Aufbewahrung und Verwendung bzw. der Weitergabe von Daten über Personen mit ein (Urteil des EGMR Wasmuth gegen Deutschland vom 17. Februar 2011, 12884/03, § 74; Urteil des EGMR Amann gegen die Schweiz vom 16. Februar 2000, 27798/95, § 46; Urteil Leander gegen Schweden vom 26. März 1987, 9248/81, § 48).

In seiner Rechtsprechung hatte sich der EGMR wiederholt damit zu befassen, inwieweit (geheime) staatliche Überwachungsmassnahmen mit den Garantien gemäss Art. 8 EMRK vereinbar sind bzw. wie weit der Schutzbereich von Art. 8 EMRK in dieser Hinsicht reicht. Er geht seit dem Urteil Klass und andere gegen Deutschland davon aus, dass bereits die blosse Existenz von Gesetzen, die eine geheime Überwachung etwa des Fernmeldeverkehrs ermöglichen, für alle möglicherweise von dem Gesetz Betroffenen ein Überwachungsrisiko beinhaltet, die Vertraulichkeit der Kom-

munikation beeinträchtigt und aus diesem Grund einen Eingriff in die gemäss Art. 8 Ziff. 1 EMRK garantierten Rechte darstellt. Er erwog Folgendes (Urteil des EGMR Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, § 36):

> La Cour ne saurait admettre que l'assurance de bénéficier d'un droit garanti par la Convention puisse être ainsi supprimée du simple fait de maintenir l'intéressé dans l'ignorance de sa violation.

Der EGMR lässt somit grundsätzliche eine potentielle Verletzung der garantierten Rechte genügen und prüft die betreffenden Erlasse abstrakt, ohne dass eine tatsächliche Beeinträchtigung nachgewiesen sein müsste (Urteil Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, § 41). In seiner jüngeren Rechtsprechung hat der EGMR das erwähnte Urteil Klass und andere gegen Deutschland präzisiert. Demnach genügt die blosse Existenz geheimer Überwachungsmassnahmen bzw. entsprechender gesetzlicher Bestimmungen für eine Verletzung der konventionsrechtlichen Garantien, wenn die Beschwerde führende Person von der Massnahme zumindest möglicherweise betroffen ist, etwa weil die Massnahme alle Nutzer einer Kommunikationsdienstleistung betrifft; der EGMR spricht von einem virtuellen Eingriff in die konventionsrechtlichen Garantien. Zudem bezieht der EGMR die Möglichkeit innerstaatlicher Rechtsmittel, die gegen die Überwachungsmassnahme erhoben werden können, mit in seine Betrachtung ein (Urteil des EGMR Roman Zakharov gegen Russland vom 4. Dezember 2015, 47143/06, §§ 164–171; Urteil des EGMR Kennedy gegen Vereinigtes Königreich vom 18. Mai 2010, 26839/05, § 124; vgl. auch Urteil des EGMR Szabó und Vissy gegen Ungarn vom 12. Januar 2016, 37138/14, § 53). Im Urteil Roman Zakharov gegen Russland schloss der EGMR mit der Feststellung (Urteil des EGMR Roman Zakharov gegen Russland vom 4. Dezember 2015, 47143/06, § 172):

> L'approche définie dans l'arrêt Kennedy offre donc à la Cour la souplesse nécessaire pour traiter tous les types de situations qui peuvent se présenter en matière de surveillance secrète eu égard aux spécificités des ordres juridiques des États membres, c'est-à-dire les recours existants, ainsi qu'à la situation personnelle de chaque requérant.

Die Entscheidung darüber, ob die gespeicherten personenbezogenen Informationen einen Aspekt des Privatlebens betreffen, erfolgt somit einzelfallbezogen. Ein wichtiges Kriterium hierbei sind die Erwartungen einer Person im Hinblick auf ihr Privatleben wie auch im Hinblick auf die Vertraulichkeit ihrer Kommunikation. Darüber hinaus sind nebst den Umständen

der Speicherung insbesondere die Art der Aufzeichnung, die Art einer allfälligen Verwendung, die Art der Verarbeitung, die Ergebnisse, die erlangt werden können, sowie der Charakter der Daten zu berücksichtigen (zum Ganzen Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010, 35623/05, §§ 43-48 mit Hinweisen und einer Zusammenfassung der bisherigen Rechtsprechung; vgl. zudem Urteil des EGMR S. und Marper gegen Vereinigtes Königreich vom 4. Dezember 2008, 30562/04 und 30566/04, §§ 67–86; Urteil des EGMR Copland gegen Vereinigtes Königreich vom 3. April 2007, 62617/00, §§ 43 f.; Urteil des EGMR Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, § 41; ferner BGE 138 I 6 E. 4.1 mit Hinweisen auf die Rechtsprechung des EGMR). So ging der EGMR davon aus, das systematische Sammeln und Speichern von Daten bestimmter Personen stelle einen Eingriff in das Privatleben dieser Personen dar (Urteil Uzun gegen Deutschland vom 2. September 2010, 35623/05, §§ 44–47; vgl. auch das Urteil des EGMR Rotaru gegen Rumänien vom 4. Mai 2000, 28341/95, § 43, in welchem die Speicherung von Informationen zu beurteilen war, welche die weit zurückliegende Vergangenheit einer Person betrafen). Ob die Daten zu einem späteren Zeitpunkt tatsächlich verwendet werden, ist für die Feststellung unerheblich (Urteil des EGMR S. und Marper gegen Vereinigtes Königreich vom 4. Dezember 2008, 30562/04 und 30566/04, § 67).

In ständiger Rechtsprechung weist der EGMR sodann darauf hin, dass der Schutzbereich der Privatsphäre nicht (ohne Weiteres) endet, wenn eine Person aus dem Kreis ihrer Privatsphäre hinaus in die Öffentlichkeit tritt. Zum Schutzumfang von Art. 8 EMRK gehört etwa, sich grundsätzlich ohne Beobachtung durch staatliche Organe im öffentlichen Raum bewegen zu können. Für die Beurteilung, ob eine staatliche (Überwachungs-)Massnahme den sachlichen Schutzbereich von Art. 8 EMRK tangiert, stellt der Gerichtshof nebst anderen Elementen insbesondere darauf ab, ob die betroffene Person (nach den konkreten Umständen) auch im öffentlichen Raum in begründeter Weise erwarten kann, vom Schutzbereich der Privatsphäre erfasst zu sein ("pouvait raisonnablement croire au caractère privé"; Urteil des EGMR Peev gegen Bulgarien vom 26. Juli 2007, 64209/01, §§ 38 f.; im gleichen Sinn Urteil des EGMR Gillan und Quinton gegen Vereinigtes Königreich vom 12. Januar 2010, 4158/05, § 61; Urteil des EGMR P.G. und J.H. gegen Vereinigtes Königreich vom 25. September 2001, 44787/98, § 57; vgl. auch SIGRIST, a.a.O., S. 44 f.; Urteil des EGMR Halford gegen Vereinigtes Königreich vom 25. Juni 1997, 20605/92, § 45). So durfte etwa ein Arbeitnehmer erwarten, dass auch in Bezug auf seinen Arbeitsplatz – jedenfalls bezüglich Schreibtisch und Aktenmöbel – seine

Privatsphäre respektiert wird (Urteil des EGMR Peev gegen Bulgarien vom 26. Juli 2007, 64209/01, §§ 38 f.). Nach der Rechtsprechung des EGMR fällt zudem die verdeckte Aufzeichnung von Telefongesprächen in den Anwendungsbereich von Art. 8 EMRK, und zwar hinsichtlich beider Aspekte des in Art. 8 EMRK garantierten Rechts, nämlich der Achtung des Privatlebens wie auch der Korrespondenz (Urteil des EGMR Liberty und andere gegen Vereinigtes Königreich vom 1. Juli 2008, 58243/00, § 56 unter Verweis auf das Urteil des EGMR Weber und Saravia gegen Deutschland vom 29. Juni 2006, 54934/00, § 77; Urteil des EGMR P.G. und J.H. gegen Vereinigtes Königreich vom 25. September 2001, 44787/98, § 59; vgl. zudem zur Überschneidung der Schutzbereiche GRABENWARTER/PABEL, a.a.O., § 22 Rz. 10). Entsprechend durfte eine Arbeitnehmerin erwarten, dass von ihrem Arbeitsplatz aus geführte Telefongespräche gleich wie der Versand von E-Mails und die Nutzung des Internets als Teil der Privatsphäre angesehen werden (Urteil des EGMR Copland gegen Vereinigtes Königreich vom 3. April 2007, 62617/00, § 42; vgl. zum Ganzen die zusammenfassende Darstellung der Rechtsprechung bei BIRTE SIEMEN, Datenschutz als Europäisches Grundrecht, 2006, S. 121–129).

9.2.3 Die Beschwerdeführer berufen sich schliesslich auf Art. 17 UNO-Pakt II. Demnach darf niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden (Ziff. 1). Nach Ziff. 2 hat zudem jedermann Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen. Vorliegend ist jedoch nicht ersichtlich, dass diese Bestimmung weitergehende Ansprüche einräumt bzw. einen weitergehenden Schutz als jenen gemäss Art. 8 EMRK gewährt (BGE 139 II 404 E. 7.1 mit Hinweisen). Es rechtfertigt sich daher, die Vorbringen der Beschwerdeführer im Folgenden im Lichte von Art. 13 BV und Art. 8 EMRK zu prüfen. Dabei ist die dargestellte Rechtsprechung von Bundesgericht und EGMR insoweit zu berücksichtigen, als es mit Blick auf die Trennung von Verwaltungs- und Strafverfahren sachgerecht erscheint.

9.3 Der sachliche Schutzbereich des Fernmeldegeheimnisses i.S.v. Art. 13 Abs. 1 BV ist, wie vorstehend erwogen, auf die fernmeldetechnische Kommunikation bzw. den Kommunikationsvorgang beschränkt. Es fragt sich daher und ist im Folgenden zu prüfen, ob sämtliche Daten, welche gemäss den unbestritten gebliebenen Ausführungen der Beschwerdeführer gespeichert werden und soweit deren Speicherung und Aufbewahrung im Streit

liegt, überhaupt in den sachlichen Schutzbereich des Fernmeldegeheimnisses fallen.

Vorab ist festzuhalten, dass der Schutzbereich des Fernmeldegeheimnisses – wie auch jener des Rechts auf informationelle Selbstbestimmung – technikneutral ist. Geschützt ist mithin jede fernmeldetechnische Kommunikation, unbesehen des verwendeten Kommunikationsmittels (vgl. BGE 126 I 50 E. 6a; zudem SIGRIST, a.a.O., S. 46). In den Schutzbereich fallen somit zunächst jene Daten, welche im Zusammenhang mit einer fernmeldetechnischen Kommunikation von den Anbieterinnen bearbeitet werden bzw. bei diesen anfallen. Gemeint sind insbesondere der Zeitpunkt der Kommunikation bzw. der Datenverbindung und deren Dauer, die Art der Datenverbindung und bei der Überwachung des E-Mail-Verkehrs das benutzte Protokoll (vgl. Art. 16 Bst. d Ziff. 4, Art. 24b Bst. a Ziffn. 1 und 2 sowie Bst. b Ziffn. 1 und 2 VÜPF). Diese Randdaten sind nach der Rechtsprechung durch das Fernmeldegeheimnis geschützt (vgl. vorstehend E. 9.2 sowie BONDALLAZ, a.a.O., Rz. 1098).

Ebenfalls in den Schutzbereich des Fernmeldegeheimnisses fallen weitere, mit einem Fernmeldevorgang verbundene Daten wie etwa die Adressierungselemente. Adressierungselemente sind nach Art. 3 Bst. f und g FMG Elemente zur Identifikation von Personen, Computerprozessen, Maschinen und Geräten oder Fernmeldeanlagen wie Kennzahlen, Rufnummern und Kurznummern. Dazu zählen u.a. Telefonnummern, IP-Adressen, Domain-Namen, die IMEI- und die IMSI-Nummer sowie die MAC-Adresse (vgl. Art. 16 Bst. d Ziffn. 1 und 2, Art. 24b Bst. a Ziffn. 4 und 5 sowie Bst. b Ziffn. 3 und 4 VÜPF). Ausserhalb eines Kommunikationsvorgangs handelt es sich um Bestandesdaten, welche grundsätzlich in einem vereinfachten Verfahren abgefragt werden können (vgl. vorstehend E. 4.2; BONDALLAZ, a.a.O., Rz. 1798). Im Falle einer konkreten fernmeldetechnischen Übertragung hingegen dienen die Adressierungselemente der Identifikation der teilnehmenden Anschlüsse und (damit) der Teilnehmer. Sie erlauben insofern das Stattfinden der Telekommunikation, lassen sich dieser mithin unmittelbar zuordnen und fallen in diesem Kontext ebenfalls in den sachlichen Schutzbereich des Fernmeldegeheimnisses (BERANEK ZANON/DE LA CRUZ BÖHRINGER, a.a.O., Rz. 9.67 ff. mit Hinweisen; WEBER/SOMMERHALDER, Das Recht der personenbezogenen Information, 2007, S. 51 f. und 57 f.). Dynamische IP-Adressen werden bei jeder Verbindungsaufnahme neu zugewiesen. Sie ermöglichen so erst die Kommunikation und fallen somit mit der Zuweisung unter das Fernmeldegeheimnis (BONDALLAZ, a.a.O.,

Rz. 1100 mit Hinweisen; WEBER/SCHNYDER, "Was für 'ne Sorte von Geschöpf ist Euer Krokodil?", zur datenschutzrechtlichen Qualifikation von IP-Adressen, sic! 2009, S. 570 f.).

Nicht unumstritten ist die Zuordnung weiterer (technischer) Daten wie etwa Angaben zum PUK (Personal Unblocking Key) oder darüber, ob und unter welcher Nummer bzw. mit welcher SIM-Karte ein bestimmtes mobiles Gerät bei einer bestimmten Anbieterin betrieben wird. Nach der Rechtsprechung des Bundesgerichts handelt es sich grundsätzlich um Bestandesdaten, die unabhängig von einem bestimmten Fernmeldeverkehr vorhanden sind bzw. diesen nicht betreffen und mithin nicht dem Fernmeldegeheimnis unterliegen (BGE 141 IV 423 E. 1.3 mit Hinweisen auf die [abweichende] Literatur; vgl. auch Botschaft nBÜPF, BBl 2013 2683, 2734, wonach der Bundesrat die Kompetenz erhalten soll, die Anbieterinnen zur Erteilung weiterer Auskünfte über Bestandesdaten wie etwa den PUK zu verpflichten). Dieses Verständnis entspricht – jedenfalls wenn kein Kommunikationsvorgang betroffen ist und die Bestandesdaten i.S.v. Art. 14 Abs. 1 BÜPF isoliert abgefragt werden – den Festlegungen in Art. 2 Gebührenposition A 1 der Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF, SR 780.115.1). Zudem finden technische Daten wie etwa der PUK – anders als die Adressierungselemente – keine Erwähnung in Art. 16 Bst. d VÜPF, welcher die im Rahmen der rückwirkenden Überwachung zu liefernden Daten festlegt (vgl. jedoch Art. 24b Bst. a Ziff. 3 VÜPF, wonach im Zusammenhang mit der Überwachung des Internets auch die verwendeten Anmeldedaten [Log-in] zu liefern sind). Vorliegend ist somit davon auszugehen, dass technische Angaben wie etwa der von den Beschwerdeführern ausdrücklich erwähnte PUK keine Randdaten darstellen, welche gestützt auf Art. 15 Abs. 1 und 3 BÜPF zu speichern und auf Verlangen hin der Staatsanwaltschaft zuzuleiten sind. Die Frage, ob diese Daten ebenfalls in den Schutzbereich des Fernmeldegeheimnisses fallen, kann daher offen bleiben.

Moderne (mobile) Telekommunikationsmittel erzeugen automatisch Daten etwa zum Standort und zum Status eines (mobilen) Geräts. Standortdaten werden automatisch und kontinuierlich erzeugt, wenn das Gerät des Benutzers eingeschaltet ist. Sie geben – das Mobilfunknetz betreffend – in geografischer Hinsicht Auskunft darüber, innerhalb welcher Funkzelle sich ein Gerät befindet bzw. zuletzt befand. Zudem werden Statusinformationen übermittelt, also beispielsweise Informationen darüber, ob ein Gerät einge-

schaltet bzw. empfangsbereit ist oder nicht. Die Anbieterinnen sind verpflichtet, den Zell-Identifikator (Cell-ID), den Standort und die Hauptstrahlrichtung derjenigen Antenne, mit der ein Endgerät zum Zeitpunkt der Kommunikation verbunden ist, zu speichern und aufzubewahren (vgl. Art. 16 Bst. d Ziff. 3 und Bst. e, Art. 24b Bst. a Ziff. 6 VÜPF). Fallen diese Daten im Zusammenhang mit einem Fernmeldeverkehr an, beispielsweise bei einem Anruf, dem Erhalt einer E-Mail und dem Versenden einer Twitter-Nachricht, sind sie mit Blick auf die Achtung des umfassend zu verstehenden Fernmeldeverkehrs ebenfalls vom sachlichen Schutzbereich von Art. 13 Abs. 1 BV erfasst (BONDALLAZ, a.a.O., Rz. 1098 f. mit Hinweisen). Andernfalls, d.h. ohne Bezug zu einem Fernmeldeverkehr, müssen und dürfen Angaben zum Standort und zum Status eines (mobilen) Geräts gestützt auf Art. 15 Abs. 3 BÜPF nicht gespeichert werden (Art. 16 Bst. d Ziff. 3 und Bst. e sowie Art. 24b Bst. a Ziff. 6 VÜPF e contrario). Ein Zuleiten entsprechender Daten an die Vorinstanz gestützt auf Art. 15 Abs. 1 BÜPF und eine Herausgabe an die Strafverfolgungsbehörden steht daher von vornherein nicht in Frage. Somit kann vorliegend offen bleiben, ob entsprechende Daten, die ausserhalb eines Kommunikationsvorgangs gespeichert werden, ebenfalls in den Schutzbereich des umfassend zu verstehenden Fernmeldegeheimnisses fielen oder durch das Recht auf informationelle Selbstbestimmung i.S.v. Art. 13 Abs. 2 BV geschützt wären (vgl. BONDALLAZ, a.a.O., Rz. 1099 und 1107, welcher einen Schutz entsprechender Daten durch das Fernmeldegeheimnis [im Ergebnis] mit der Begründung verneint, die automatische Kommunikation zwischen einem [mobilen] Gerät und der Anbieterin zwecks Lokalisierung und Übermittlung von Statusinformationen sei kein durch Art. 13 Abs. 1 BV erfasster Fernmeldeverkehr; demgegenüber wohl HANSJAKOB, Kommentar BÜPF / VÜPF, S. 88 f., wonach die laufende Standortidentifikation den Fernmeldeverkehr betrifft, da die Anbieterinnen bzw. die Netzbetreiberinnen die technische Information über den Standort brauche, um ankommenden Fernmeldeverkehr richtig leiten zu können).

Die Beschwerdeführer wenden sich gegen die Speicherung und Aufbewahrung von (Rand-)Daten betreffend ihre Kommunikation. In ihren Rechtsbegehren nehmen sie ausdrücklich jene Daten aus, welche für die Erbringung der vertraglichen Leistungen durch die Anbieterinnen erforderlich sind. Entsprechend steht das Speichern und Aufbewahren von Personendaten über die Kundenbeziehung, wie etwa Angaben zum Inhaber eines Anschlusses und zur Bezahlung der erbrachten Dienstleistungen, vorliegend nicht in Frage. Ob diese Daten unter Einhaltung der gesetzlichen Vorgaben im Rahmen der Überwachung des Post- und Fernmeldeverkehrs etwa an die

Strafverfolgungsbehörden herausgegeben werden dürfen, ist – wie vorstehend bereits festgehalten – überdies nicht im Rahmen des vorliegenden Beschwerdeverfahrens zu beurteilen (vgl. vorstehend E. 8; zudem BONDALLAZ, a.a.O., Rz. 1101, wonach Kundendaten, wenn sie zusammen mit weiteren Randdaten mitgeteilt werden, ebenfalls dem Fernmeldegeheimnis unterliegen). Die weiteren Randdaten, die von den Anbieterinnen gespeichert werden und Auskunft darüber geben, wer mit wem, wann, wie lange und von wo aus kommuniziert hat sowie die technischen Details der entsprechenden Verbindung, fallen jedoch nach dem vorstehend Ausgeführten in den Schutzbereich des Fernmeldegeheimnisses. Dasselbe gilt für die versuchte, jedoch nicht zu Stande gekommene Kommunikation. Im Folgenden ist somit zu prüfen, ob in das grundrechtlich geschützte Fernmeldegeheimnis eingegriffen wird, indem die Randdaten der Telekommunikation der Beschwerdeführer gespeichert und (eine beschränkte Zeit lang) aufbewahrt werden.

9.4 Vorliegend sind die folgenden konkreten Umstände wesentlich: Die Bestimmung von Art. 15 Abs. 3 BÜPF verpflichtet die Anbieterinnen zu einer systematischen Speicherung und Aufbewahrung von Randdaten der Telekommunikation (der Beschwerdeführer). Betroffen sind personenbezogene Daten von grossem Umfang, aus denen über einen längeren Zeitraum hervorgeht, mit wem, wann, wie lange und von wo aus die Beschwerdeführer kommuniziert haben (zur Qualifikation von Daten als Personendaten BERANEK ZANON/DE LA CRUZ BÖHRINGER, a.a.O., Rz. 9.81; vgl. zudem BGE 128 II 259 E. 3.2; Urteil des EGMR S. und Marper gegen Vereinigtes Königreich vom 4. Dezember 2008, 30562/04 und 30566/04, § 83; zudem SIGRIST, a.a.O., S. 49). Eingeschlossen ist auch die (mobile) Nutzung des Internets. Diese Angaben können – trotzdem es sich "lediglich" um die äusseren Daten der Kommunikation handelt – zu Persönlichkeitsprofilen über die Kommunikation der Beschwerdeführer bzw. über deren äussere Umstände verdichtet werden, an deren Bearbeitung der Gesetzgeber erhöhte Anforderungen stellt (Art. 17 Abs. 2 DSG; vgl. BGE 138 II 346 E. 8.2; DIGGELMANN, a.a.O., Art. 13 Rz. 29; ROLF H. WEBER, Fernmeldegeheimnis, S. 198; ferner Urteil des deutschen Bundesverfassungsgerichts 1 BvR 256/08 vom 2. März 2010 Rz. 209–212, abrufbar unter < www.bundesverfassungsgericht.de > Entscheidungen > vor 2012 > 2010 > März [besucht am 25. Oktober 2016]; BIRGIT KOLB, Vorratsdatenspeicherung, 2011, S. 104 f.; zudem zu Art. 17 Abs. 2 Bst. a DSG das Urteil des BGer 6B_4/2011 vom 28. November 2011 E. 2.8); als Persönlichkeitsprofil gilt nach Art. 3 Bst. d DSG eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person

erlaubt. Die Randdaten lassen in ihrer Gesamtheit ohne Weiteres Rückschlüsse auf die persönlichen Lebensverhältnisse und das persönliche Umfeld zu (vgl. BGE 138 II 346 E. 6.3). Zudem erfolgt die Speicherung und Aufbewahrung der Randdaten ohne konkreten Anlass, d.h. es ist insbesondere nicht erforderlich, dass gegen die betroffene Person bereits ein Vorverfahren i.S.v. Art. 299 StPO eingeleitet worden ist (vgl. BGE 140 I 381 E. 4.5.1; zudem BGE 138 II 346 E. 10.6.1).

Die Speicherung und Aufbewahrung der Randdaten durch die Anbieterinnen schränkt die Herrschaft der Beschwerdeführer über ihre personenbezogenen Daten und somit ihr Recht auf informationelle Selbstbestimmung wie auch ihren Anspruch auf Vertraulichkeit ihrer Kommunikation ein (vgl. auch das Urteil des deutschen Bundesverfassungsgerichts 1 BvR 256/08 vom 2. März 2010 Rz. 188–191). Die Beschwerdeführer dürfen vernünftigerweise erwarten, dass die Anbieterinnen nur speichern, was zur Vertragserfüllung benötigt wird und diese Daten gelöscht werden, sollten sie hierfür nicht mehr benötigt werden. Darüber geht die gesetzliche Pflicht von Art. 15 Abs. 3 BÜPF, die Randdaten der Telekommunikation zu speichern und während sechs Monaten aufzubewahren, jedoch unstrittig hinaus. Hinzu kommt, dass der Eingriff mit der Aufbewahrung der Randdaten (im Hinblick auf eine allfällige Verwendung) aufrechterhalten und zusätzlich noch verschärft wird (BGE 137 I 167 E. 3.2; BGE 123 IV 236 E. 4; SIGRIST, a.a.O., S. 98 f.; vgl. zudem BGE 133 I 77 E. 5.3 zur Berücksichtigung der Dauer der Aufbewahrung bei der Beurteilung der Schwere einer Grundrechtseinschränkung).

Gegen das Vorliegen einer Grundrechtseinschränkung lässt sich einwenden, dass die Speicherung und Aufbewahrung von Randdaten nicht heimlich erfolgt und im Zeitpunkt der Speicherung der Randdaten unsicher und in den allermeisten Fällen gar unwahrscheinlich ist, dass diese je den Strafverfolgungsbehörden bekannt gegeben werden (müssen) bzw. je – etwa in einem Strafverfahren – verwendet werden. Darauf kommt es nach der Rechtsprechung aber auch nicht an. Es ist unerheblich, ob gespeicherte Daten zu einem späteren Zeitpunkt etwa in einem Strafverfahren verwendet werden, da bereits die Speicherung und Aufbewahrung für sich einen Eingriff in die geschützte Privatsphäre bzw. das Recht auf informationelle Selbstbestimmung darstellt. Zudem ist auf das Folgende hinzuweisen: Die Anbieterinnen haben die Randdaten gestützt auf eine Anordnung der Staatsanwaltschaft der Vorinstanz zuzuleiten (Art. 15 Abs. 1 BÜPF). Die Vorinstanz wiederum hält die Randdaten der anordnenden Strafverfol-

gungsbehörde zur Verfügung bzw. sendet ihr die Randdaten zu. Eine Genehmigung der rückwirkenden Überwachungsanordnung durch das Zwangsmassnahmengericht liegt zu diesem Zeitpunkt in der Regel noch nicht vor und Betroffenen steht noch kein Rechtsmittel gegen die Überwachungsanordnung offen. Das Zwangsmassnahmengericht entscheidet nach Art. 274 Abs. 2 und 3 StPO innert fünf Tagen seit der Anordnung der Überwachung, während die Zuleitung der Randdaten in der Regel sofort bzw. innert kurzer Zeit erfolgt. Der beschuldigten Person wird die Überwachung erst nachträglich, spätestens mit Abschluss des Vorverfahrens, mitgeteilt, wobei die Mitteilung u.U. auch unterlassen werden kann (Art. 279 Abs. 1 und 2 StPO). Entsprechend steht ihr auch erst – wenn die Mitteilung nicht unterlassen wird – nachträglich ein Rechtsmittel gegen die Überwachung zu (Art. 279 Abs. 3 StPO). Zwar sind die Dokumente und Datenträger aus einer (nachträglich) nicht genehmigten oder für unzulässig erklärten Überwachung sofort zu vernichten und durch die Überwachung gewonnene Erkenntnisse dürfen nicht verwendet werden. Für die Beurteilung, ob ein Eingriff in das grundrechtlich geschützte Fernmeldegeheimnis vorliegt, ist dies aber nicht relevant. Das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung sind – im Fall etwa der Anordnung einer geheimen rückwirkenden Überwachung des Fernmeldeverkehrs – bereits mit der blossen und in diesem Moment geheimen Bekanntgabe der Randdaten (zusätzlich) verletzt, da in diesem Fall Dritte von den Randdaten Kenntnis nehmen (vgl. JENT-SØRENSEN/KATZENSTEIN/KELLER, Telefonüberwachung – Verfassungsrechtliche Vorgaben und praktische Umsetzung, in: Individuum und Verband, Festgabe zum Schweizerischen Juristentag 2006, 2006, S. 553). Ob diese Kenntnisnahme und die aus der Überwachung gewonnenen Erkenntnisse später allenfalls einem strafprozessualen Verwertungsverbot unterliegen, ist hierfür unerheblich; die Kenntnisnahme wird durch ein Verwertungsverbot nicht wieder rückgängig gemacht (vgl. BGE 109 Ia 273 E. 12a).

Die Speicherung und Aufbewahrung von Randdaten ist schliesslich nicht Selbstzweck, sondern Voraussetzung insbesondere für die Anordnung einer rückwirkenden Überwachung des Fernmeldeverkehrs im Rahmen der Strafverfolgung; die Randdaten werden insbesondere zu diesem Zweck gespeichert und aufbewahrt (Art. 1 Abs. 1 Bst. a BÜPF). Es rechtfertigt sich daher, die vorstehend dargestellte Rechtsprechung des EGMR zu (geheimen) Überwachungsmassnahmen sinngemäss auch auf die vorliegende Streitsache anzuwenden, selbst wenn konkret keine Überwachungsmassnahme im Streit liegt bzw. zu beurteilen ist (vgl. SIEMEN, a.a.O., S. 101–103; KOLB, a.a.O., S. 121). Demnach genügt grundsätzlich ein virtueller

Eingriff bzw. die blosse Existenz geheimer Überwachungsmassnahmen für eine Verletzung der konventionsrechtlich geschützten Privatsphäre, wenn die Beschwerde führende Person von der Massnahme zumindest möglicherweise betroffen ist, etwa weil die Massnahme alle Nutzer einer Kommunikationsdienstleistung betrifft (vgl. vorstehend E. 9.2; zudem BVGE 2009/46 E. 8.3; Urteil des EGMR Kopp gegen Schweiz vom 25. März 1998, 13/1997/797/1000, § 53; JENS MEYER-LADEWIG, Handkommentar EMRK, 3. Aufl. 2011, Art. 8 Rz. 42). In diesem Zusammenhang wird auch davon gesprochen, dass bereits die Möglichkeit einer späteren, zunächst geheimen Verwendung der Randdaten (in einer Strafuntersuchung) Einfluss auf das persönliche Verhalten haben kann, indem ein diffuses Gefühl des Überwacht- bzw. Beobachtet-Werdens entsteht (sog. Chilling Effect, vgl. hierzu ausführlich SIGRIST, a.a.O., S. 108 und BGE 113 Ia 1 E. 4b/bb; zur Heimlichkeit der Überwachung vorstehend E. 9.2 und MOOR/STUDER, Randdatenerhebung bei Vorliegen der Einwilligung sowie bei Dritten, Jusletter vom 30. Mai 2016, Rz. 31 f.). Die Möglichkeit der Verwendung der Randdaten in einem späteren Strafverfahren begründet daher vorliegend eine weitere Betroffenheit in grund- und völkerrechtlich geschützte Rechtspositionen und wirkt insofern zusätzlich eingriffsbegründend und –erschwerend. Schliesslich ist darauf hinzuweisen, dass mit Blick auf den Zweck, zu welchem die Randdaten der Telekommunikation gespeichert und aufbewahrt werden, für die Frage der Grundrechtseinschränkung grundsätzlich ohne Bedeutung bleiben muss, dass die Daten bei bzw. von den Anbieterinnen gespeichert werden; aus Sicht des Grundrechtsschutzes erscheint dies – ein fehlender unmittelbarer Zugriff des Staates auf die Randdaten – gar geboten.

Im Ergebnis ist somit davon auszugehen, dass die Speicherung und Aufbewahrung von Randdaten der Telekommunikation i.S.v. Art. 15 Abs. 3 BÜPF einen schweren Eingriff in das Recht der Beschwerdeführer auf Achtung ihres Fernmeldeverkehrs (Art. 13 Abs. 1 BV und Art. 8 Ziff. 1 EMRK) und ihres Rechts auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Ziff. 1 EMRK) darstellt, umso mehr als beide Garantien auch für die Meinungs- und Versammlungsfreiheit von grundlegender Bedeutung sind (vgl. nachfolgend E. 9.6). Dieses Ergebnis – ein Eingriff in die betreffenden Schutzbereiche – wird nach der Rechtsprechung des EGMR durch das Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SR 0.235.1, für die Schweiz in Kraft getreten am 1. Februar 1998, nachfolgend: Datenschutzkonvention) bekräftigt (vgl. SIEMEN, a.a.O., S. 121 mit Hinweisen).

Anzumerken ist, dass es für die Beurteilung, ob ein Eingriff in grundrechtlich geschützte Positionen vorliegt, grundsätzlich ohne Belang ist, ob die Speicherung und Aufbewahrung von Randdaten und damit der Eingriff in das Grundrecht als im öffentlichen Interesse liegend gerechtfertigt werden kann. Die Frage der allfälligen Rechtfertigung einer Einschränkung ist Gegenstand einer späteren Prüfung (vgl. nachfolgend E. 10 ff.).

9.5 Die Speicherung und Aufbewahrung von Randdaten greift nach dem Gesagten gleichermassen in die grundrechtlich geschützte Vertraulichkeit der Kommunikation (Art. 13 Abs. 1 BV) wie auch in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) ein. Es fragt sich daher, ob der vorliegend zu beurteilende Sachverhalt einem der beiden berührten Grundrechte zuzuordnen und lediglich dieser eine Grundrechtseingriff auf seine Rechtfertigung hin zu prüfen ist. Dies ist zu verneinen. Beide berührten Grundrechte haben – auch wenn sich die Schutzbereiche der beiden Grundrecht mit Blick auf deren Beitrag zur Persönlichkeitsentfaltung überschneiden – eine auf einen speziellen Schutz ausgerichtete Bedeutung. Das Fernmeldegeheimnis schützt die Vertraulichkeit der Kommunikation, während in Art. 13 Abs. 2 BV der Datenschutz eine grundrechtliche Verankerung findet. Letzterem kommt vorliegend unstreitig ein erhebliches Gewicht zu (vgl. auch nachfolgend E. 12.8). Es kann somit nicht gesagt werden, der inhaltliche Tatbestand des Fernmeldegeheimnisses überwiege den Anspruch auf informationelle Selbstbestimmung klar (vgl. SCHWEIZER, a.a.O., Art. 36 Rz. 4). Davon geht auch der EGMR in konstanter Rechtsprechung aus; das Speichern von Randdaten der Telekommunikation stellt demnach einen Eingriff sowohl in das Recht auf Privatleben bzw. die Privatsphäre wie auch in das Recht auf Achtung der Korrespondenz dar (kombinierter Schutzbereich), zumal keine (erheblichen) Unterschiede bezüglich der Schranken der beiden Freiheitsrechte auszumachen sind (vgl. vorstehend E. 9.2; BASIL CUPA, Rechtsschutz gegen präventive Überwachungsmassnahmen am Beispiel des Nachrichtendienstes des Bundes [NDB], 2014, Rz. 113 f.; im Ergebnis auch SCHLAURI/RONZANI; EuGH: Vorratsdatenspeicherungsrichtlinie 2006/24/EG für ungültig erklärt, in: sic! [Zeitschrift für Immaterialgüter, Informations- und Wettbewerbsrecht] 2014 S. 575). Es ist daher vorliegend gesamthaft, d.h. unter Berücksichtigung beider Grundrechtsinteressen, zu prüfen, ob der Eingriff vor der Verfassung und der EMRK stand hält (vgl. in diesem Zusammenhang BELSER, a.a.O., § 6 Rz. 157 ff. mit Hinweisen auf die Rechtsprechung und Literatur).

9.6 Die Beschwerdeführer rufen mit der persönlichen Freiheit (Art. 10 Abs. 2 BV, Art. 8 EMRK) sowie der Meinungs- und Versammlungsfreiheit

(Art. 16 und Art. 22 BV, Art. 10 und Art. 11 EMRK) weitere Grundrechte an, die durch die Speicherung und Aufbewahrung von Randdaten ihrer Telekommunikation verletzt sein sollen.

Nach der Rechtsprechung und der Lehre gehen die speziellen Freiheitsrechte von Art. 13 BV der allgemeineren Garantie der persönlichen Freiheit vor, wenn wie vorliegend nicht die körperliche Integrität oder individuelle Aspekte der Lebensgestaltung, sondern ein Eingriff in die Privatsphäre in Frage steht (im Ergebnis BGE 133 I 77, E. 3.2; BGE 128 II 259 E. 3.2; BGE 126 I 50 E. 5a; DIGGELMANN, a.a.O., Art. 13 Rz. 10; BELSER, a.a.O., § 6 Rz. 158 f. und 164–167). Auf Art. 10 Abs. 2 BV ist daher vorliegend nicht näher einzugehen.

Die Meinungsfreiheit schützt die freie bzw. ungehinderte Bildung, Äusserung und Verbreitung von Meinungen, wobei von einem weiten Begriff der Meinung auszugehen ist. Geschützt ist auch die freie Wahl von Kommunikationsform und –mittel (vgl. zum Schutzbereich KLEY/TOPHINKE, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 16 Rz. 5 ff.). Zur Verwirklichung der Meinungsfreiheit ist die Vertraulichkeit der Kommunikation von besonderer Bedeutung; die Überwachung der Telekommunikation kann den einzelnen von einer Meinungskundgabe abschrecken (vgl. zum Chilling Effect vorstehend E. 9.4; zudem MÜLLER/SCHEFER, a.a.O., S. 375 f.). Vorliegend stehen mit der Speicherung der Randdaten allerdings die äusseren Umstände der Kommunikation und nicht deren Inhalt in Frage. Vor diesem Hintergrund ist das Fernmeldegeheimnis, dessen Gewährleistungsbereich die Vertraulichkeit der Kommunikation ist, das speziellere Grundrecht. Dies umso mehr, als sich die Beschwerdeführer eines Übertragungsmediums bedienen, auf das sich – wie vorliegend – der Staat Zugriff verschaffen kann (vgl. MÜLLER/SCHEFER, a.a.O., S. 202). Letztlich kann jedoch offen bleiben, ob die Bedeutung des Fernmeldegeheimnisses für die Meinungsfreiheit eine kumulative Berufung auf beide Grundrechte zulässt (vgl. zur Grundrechtskonkurrenz BGE 137 I 167 E. 3.7 mit Hinweis insbes. auf KLEY/VOGT, Das Problem der Grundrechtskonkurrenz, ius.full 2008 S. 132 ff., insbes. S. 134 und 136 ff.; zur Charakterisierung der Meinungsfreiheit als Auffanggrundrecht BGE 127 I 164 E. 3b und BGE 127 I 145 E. 4b). Dem Grundrechtsinteresse der Meinungsfreiheit kann im Rahmen des Fernmeldegeheimnisses Rechnung getragen werden (vgl. BGE 122 I 130 E. 2). Dasselbe gilt für die Versammlungsfreiheit, die Schutz vor staatlichen Massnahmen gegen die Einberufung, Organisation, Durchführung oder Gestaltung einer Versammlung als eine Form des Zusammen-

findens von Menschen im Rahmen mit einem weit verstandenen gegenseitig meinungsbildenden, -äussernden oder -austauschenden Zweck gewährt (vgl. zum Schutzbereich CHRISTOPH ERRASS, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 22 Rz. 9 ff.). Innerhalb der nachfolgenden Beurteilung ist daher auch der Bedeutung der Vertraulichkeit der Kommunikation für die Verwirklichung der Versammlungsfreiheit als zentrale Voraussetzung für die demokratische Willensbildung hinreichend Beachtung zu schenken.

Gesetzliche Grundlage

10.

10.1 Sowohl das Fernmeldegeheimnis wie auch das Recht auf informationelle Selbstbestimmung sind nicht absolut garantiert, sondern können nach Massgabe der Verfassung und der EMRK eingeschränkt werden (Art. 36 BV; Art. 8 Ziff. 2 EMRK). Einschränkungen von Freiheitsrechten sind demnach zulässig, wenn sie auf einer gesetzlichen Grundlage beruhen (nachfolgend E. 10.2 ff.), dem Schutz eines öffentlichen Interesses oder dem Schutz der Grundrechte Dritter dienen (nachfolgend E. 11), dem Grundsatz der Verhältnismässigkeit Rechnung tragen (nachfolgend E. 12) und nicht den Kerngehalt des betreffenden Grundrechts berühren (nachfolgend E. 12.9).

Nach Ansicht der Beschwerdeführer fehlt es bei der Einschränkung ihrer Grundrechte bereits an einer hinreichend bestimmten gesetzlichen Grundlage. Gestützt auf die Bestimmung von Art. 15 Abs. 3 BÜPF sei insbesondere nicht vorhersehbar, welche Daten zu welchem Zweck gespeichert und aufbewahrt würden.

Die in Frage stehende Bestimmung weist folgenden Wortlaut auf:

> Art. 15 Pflichten der Anbieterinnen
>
> …
>
> 3 Die Anbieterinnen sind verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren.
>
> …

Das Vorbringen der Beschwerdeführer ist im Folgenden zu prüfen, wobei – entsprechend den vorstehenden Erwägungen – von einer schweren Einschränkung grundrechtlich geschützter Rechtspositionen der Beschwerdeführer auszugehen ist.

10.2 Nach Art. 36 Abs. 1 Sätze 1 und 2 BV bedürfen Einschränkungen von Grundrechten einer gesetzlichen Grundlage; schwerwiegende Einschränkungen müssen im Gesetz selbst vorgesehen sein. Die Bestimmung präzisiert das Legalitätsprinzip und verlangt u.a. eine hinreichende und angemessene Bestimmtheit der anzuwendenden Rechtssätze. Einschränkungen sollen rechtsgleich erfolgen und staatliches Handeln voraussehbar und berechenbar sein, so dass der Einzelne sein Verhalten danach richten bzw. die freiheitsbeschränkenden Folgen seines Handelns mit hinreichender Gewissheit voraussehen kann. Das Bestimmtheitserfordernis ist indes weder absolut noch abstrakt zu verstehen; der Grad an erforderlicher Bestimmtheit lässt sich nicht allgemeingültig festlegen und der Gesetzgeber kann – auch im Sinne der geforderten generell-abstrakten Regelung sowie angesichts der Vielgestaltigkeit der Verhältnisse – nicht darauf verzichten, allgemeine und mehr oder weniger vage Begriffe zu verwenden, deren Auslegung der Rechtsanwendung überlassen werden muss (BGE 140 I 381 E. 4.4; BGE 128 I 327 E. 4.2). Blankettermächtigungen, die den Behörden völlig freie Hand lassen und sie dazu ermächtigen, von Fall zu Fall zu entscheiden, sind unzulässig (HÄFELIN/MÜLLER/UHLMANN, Allgemeines Verwaltungsrecht, 7. Aufl. 2016, Rz. 342).

Massgebend sind die Umstände des Einzelfalls. Zu berücksichtigen sind unter anderem die Vielzahl der zu ordnenden Sachverhalte, die Komplexität und die Vorhersehbarkeit der im Einzelfall erforderlichen Entscheidung, die Normadressaten, die Schwere des Eingriffs in Verfassungsrechte und die erst bei der Konkretisierung im Einzelfall mögliche und sachgerechte Entscheidung (BGE 141 I 201 E. 4.1 und BGE 139 I 280 E. 5.1, je mit Hinweisen auf die Rechtsprechung). Wiegt eine Einschränkung grundrechtlich geschützter Positionen schwer, bedarf es einer qualifizierten gesetzlichen Grundlage, einer Grundlage im Gesetz selbst. Zu beurteilen ist in diesem Fall – nebst der Bestimmtheit der Norm – auch die Normstufe und damit die demokratische Legitimation des Gesetzes (SCHWEIZER, a.a.O., Art. 36 Rz. 16 mit Hinweisen; vgl. auch IVO HANGARTNER, Bemerkungen zum Urteil des BGer 1P.358/2006 [heute publiziert in BGE 133 I 77], AJP 2007 S. 514). Besteht eine gesetzliche Grundlage, aber ist diese zu unbestimmt, so braucht es eine strengere Prüfung bei der Einhaltung des Verhältnismässigkeitsgrundsatzes (SCHWEIZER, a.a.O., Art. 36 Rz. 13 und 22 mit Hinweisen auf die Rechtsprechung). Die Unbestimmtheit einer Norm kann zudem in einem gewissen Ausmass durch verfahrensrechtliche Garantien kompensiert werden und es kommt (auch in diesem Fall) dem Grundsatz der Verhältnismässigkeit erhöhte Bedeutung zu (BGE 136 I 87 E. 3.1).

Ebenso wenig wie die grundrechtlich geschützten Ansprüche gelten auch die Garantien von Art. 8 Ziff. 1 EMRK absolut. Eingriffe sind nach Massgabe von Art. 8 Ziff. 2 EMRK mit der Konvention vereinbar. Erforderlich ist, dass eine gesetzliche Grundlage im nationalen Recht den Eingriff zu rechtfertigen vermag. Das Erfordernis "prévu par la loi" verlangt nicht nur nach einer Grundlage im innerstaatlichen Recht, sondern bezieht sich auch auf dessen Qualität ("qualité de la loi"; Urteil des EGMR Malone gegen Vereinigtes Königreich vom 2. August 1984, 8691/79, § 67). Es wird eine hinreichende Zugänglichkeit ("accessible") und Vorhersehbarkeit ("prévisible") verlangt, damit der Bürger die sich daraus für ihn ergebenden Konsequenzen in hinreichendem Mass vorhersehen kann (Urteil des EGMR Szabó und Vissy gegen Ungarn vom 12. Januar 2016, 37138/14, § 59; Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010, 35623/05, § 61; vgl. auch BGE 136 I 87 E. 3.1 mit Hinweisen auf die Rechtsprechung des EGMR). Die Anforderung, wonach schwerwiegende Einschränkungen im Gesetz selbst vorgesehen sein müssen (Art. 36 Abs. 1 Satz 2 BV), findet sich allerdings in der EMRK nicht; die EMRK geht von einem materiellen Gesetzesbegriff aus und verlangt hinsichtlich Normstufe weniger als das schweizerische Recht (SCHWEIZER, a.a.O., Art. 36 Rz. 21 und 26; KIENER/KÄLIN, a.a.O., S. 99 f.).

10.3 Das Bundesgericht hat sich verschiedentlich zu den verfassungsrechtlichen Anforderungen an die (präventive) Überwachung des Fernmeldeverkehrs geäussert und dabei auf das erhebliche Missbrauchspotential insbesondere für den Fernmeldeverkehr über das Internet hingewiesen. Demnach ist eine Überwachung des Fernmeldeverkehrs nur gestützt auf eine präzise Grundlage im Gesetz selbst zulässig. Im Gesetz muss insbesondere angegeben sein, wer überwacht werden darf, welche Verdachtsmomente und welche strafbaren Handlungen Anlass zu einer Überwachung geben können, welche Behörde die Überwachung vornehmen muss und wie lange sie dauert. Zudem sind wirksame Verfahren vorzusehen, die einen Missbrauch persönlicher Daten verhindern. So muss jede Überwachungsanordnung unverzüglich durch eine richterliche Behörde genehmigt werden, es sind Grund, Art und Dauer der Überwachungsmassnahme jedenfalls im Nachhinein der überwachten Person mitzuteilen und gegen die erfolgte Überwachung muss nach der Mitteilung die Beschwerde an eine richterliche Instanz offenstehen (MÜLLER/SCHEFER, a.a.O., S. 210–214 mit Hinweisen auf die Rechtsprechung, insbes. auf BGE 126 I 50 E. 5a und E. 6a sowie auf BGE 109 Ia 273; zudem BGE 140 I 353 E. 8.7 f.; vgl. auch Art. 269 ff. StPO; DIGGELMANN, a.a.O., Art. 13 Rz. 30 mit Hinweisen auf die Rechtsprechung).

Die bisherige Rechtsprechung des Bundesgerichts hatte – soweit ersichtlich – einzig konkrete Überwachungsmassnahmen oder die abstrakte Überprüfung kantonaler Erlasse zur Strafverfolgung und damit grundsätzlich die strafprozessualen Aspekte der Überwachung zum Gegenstand (vgl. zur Trennung der verwaltungsrechtlichen von den strafprozessualen Aspekten der Überwachung vorstehend E. 8.2). Zwar ist mit der bundesgerichtlichen Rechtsprechung im Zusammenhang mit konkreten strafprozessualen Überwachungsmassnahmen grundsätzlich davon auszugehen, dass auch die Speicherung und Aufbewahrung der Daten als deren Grundlage grundrechtskonform und gesetzmässig ist. Das Bundesgericht hat sich jedoch – soweit ersichtlich – bisher nicht ausdrücklich mit der Frage befasst, welche (grundrechtlichen) Anforderungen insbesondere auch aus Sicht des Datenschutzes an die Speicherung und Aufbewahrung von Randdaten der Telekommunikation zu stellen sind bzw. ob die bestehende verwaltungsrechtliche Normierung diesen Anforderungen genügt. Es ist somit näher zu prüfen, wie es sich damit verhält.

10.4 In ähnlicher Weise hat sich das Bundesgericht zum Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV geäussert. Demnach ist für die Bearbeitung persönlicher Daten – jedenfalls wenn von einer schwerwiegenden Einschränkung auszugehen ist – eine klare gesetzliche Grundlage erforderlich; die Bearbeitung persönlicher Daten darf nicht in das Ermessen der Behörden gestellt werden, sondern muss zumindest in den Grundzügen normativ geregelt sein. Es ist mit hinreichender Bestimmtheit im Gesetz selbst zu umschreiben, unter welchen Voraussetzungen, zu welchem Zweck und in welchem Ausmass persönliche Daten welcher Personen bearbeitet werden dürfen, wem derartige Informationen bekanntgegeben werden dürfen und wann bzw. unter welchen Voraussetzungen die Daten wieder gelöscht werden müssen (BGE 136 I 87 E. 8.3; BGE 122 I 360 E. 5d; BALLENEGGER, a.a.O., Art. 17 DSG Rz. 19 und 22; vgl. auch CLAUDIA MUND, in: Baeriswyl/Pärli, Datenschutzgesetz [DSG], 2015, Art. 17 Rz. 7; YVONNE JÖHRI, in: Handkommentar zum DSG, 2008, Art. 17 Rz. 16 f.). Betroffene haben zudem einen Anspruch auf Einsicht in amtliche Daten, welche sie persönlich betreffen (MÜLLER/SCHEFER, a.a.O., S. 168 f. mit Hinweisen auf die Rechtsprechung). Der Gesetzgeber hat bezüglich des Datenschutzes die Abgrenzung zwischen leichteren Eingriffen in die Persönlichkeitsrechte von Betroffenen und schwerwiegenden Einschränkungen i.S.v. Art. 36 Abs. 1 Satz 2 BV in Art. 17 Abs. 2 DSG gleich selbst vorgenommen, indem für die Bearbeitung besonders schützenswerter Daten und von Persönlichkeitsprofilen eine formell-gesetzliche Grundlage für erforderlich erklärt wird (BALLENEGGER, a.a.O., Art. 17 DSG Rz. 13 und 16).

10.5 Auch der EGMR hat sich in seiner Rechtsprechung wiederholt dazu geäussert, welche Anforderungen an die gesetzliche Grundlage im Zusammenhang mit (geheimen) staatlichen Überwachungsmassnahmen und der Bearbeitung von Personendaten zu stellen sind. Demnach sind die Anforderungen an die Vorhersehbarkeit im speziellen Kontext der Überwachung der Telekommunikation zum Zweck der Strafverfolgung nicht dieselben, wie wenn das Gesetz – wie etwa bei Strafbestimmungen – selbst Einschränkungen für das Verhalten des Einzelnen vorsieht. Insbesondere soll es dem Einzelnen nicht ermöglicht werden, vorherzusehen, wann die Behörde seine Kommunikation überwacht, um so sein Verhalten entsprechend anzupassen und die Überwachung zu vereiteln. Einem System der geheimen Überwachung ist jedoch die Gefahr von Missbräuchen und der Willkür – jedenfalls bis zu einem gewissen Grad – inhärent. Hinzu kommt die fehlende öffentliche Kontrolle. Nach der Rechtsprechung ist es mit Blick auf die Rechtsstaatlichkeit somit erforderlich, dass bereits die rechtliche Grundlage für sich genommen dem Einzelnen mit entsprechenden Mechanismen einen den Sachverhaltsumständen angemessenen Schutz vor willkürlichen Verletzungen des Privatlebens gewährt. Eine hinreichend bestimmte Regelung ist unerlässlich, insbesondere wegen der ständigen Weiterentwicklung der verfügbaren (Überwachungs-)Technik (Urteil des EGMR Szabó und Vissy gegen Ungarn vom 12. Januar 2016, 37138/14, §§ 55 f., 59, 62 und 68; Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010, 35623/05, §§ 61 und 63, je mit Hinweisen auf die Rechtsprechung; vgl. auch BGE 138 I 6 E. 4.2 und BGE 137 I 167 E. 3.2, je mit Hinweisen auf die Rechtsprechung des EGMR).

Der EGMR hat Mindestgarantien entwickelt, die zur Vermeidung von Machtmissbrauch in den gesetzlichen Regelungen etwa zur Überwachung oder der Bearbeitung von Personendaten enthalten sein sollen. Demnach muss das innerstaatliche Recht die *Personengruppen* festlegen, deren Kommunikation durch gerichtliche Anordnung überwacht werden darf und es ist die *Natur der Straftaten* zu bestimmen, die zur Anordnung solcher Massnahmen führen können. Zudem ist eine zeitliche Begrenzung der Massnahmen vorzusehen, es ist das *Verfahren für die Auswertung, Verwendung und Speicherung* der erlangten Daten zu umschreiben und die *Löschung* bzw. Vernichtung der gespeicherten Daten zu regeln (Urteil des EGMR Calmanovici gegen Rumänien vom 1. Juli 2008, 42250/02, §§ 118–121; Urteil des EGMR Roman Zakharov gegen Russland vom 4. Dezember 2015, 47143/06, § 231 mit Hinweisen auf die Rechtsprechung und §§ 243 ff.; vgl. auch das Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010, 35623/05, § 65 f.). In anderem Zusammenhang fordert

der EGMR, dass die Art der Informationen, welche aufgezeichnet werden dürfen, die Personenkreise, gegen welche Überwachungsmassnahmen ergriffen werden dürfen, die Umstände, unter denen solche Massnahmen getroffen werden dürfen, und das Verfahren im Gesetz geregelt sein müssen (Urteil des EGMR Rotaru gegen Rumänien vom 4. Mai 2000, 28341/95, § 57 f.).

Der EGMR weist jedoch darauf hin, dass es auch bei klarer Formulierung der gesetzlichen Bestimmungen stets ein Element richterlicher Interpretation gibt; die EMRK verbiete die allmähliche Präzisierung durch gerichtliche Auslegung nicht (Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010, 35623/05, § 62). Entsprechend hat der EGMR die Verwendung von Rechtsbegriffen wie "danger of terrorist acts" und "rescue operations" zur Umschreibung der Umstände, unter denen Überwachungsmassnahmen angeordnet werden dürfen, gemessen an Ziel und Zweck des Regelungsgegenstandes und im Kontext mit anderen Erlassen als hinreichend bestimmt anerkannt (Urteil des EGMR Szabó und Vissy gegen Ungarn vom 12. Januar 2016, 37138/14, §§ 59 und 64). Und auch die Begriffe "sécurité nationale" und "infractions graves" zeigen in hinreichender Weise die Umstände und Bedingungen auf, unter denen eine Behörde zum Ergreifen von Überwachungsmassnahmen befugt ist; der EGMR verwies dabei auf die Verwendung der Begriffe in der nationalen sowie internationalen Gesetzgebung und auf die erläuternden Bestimmungen (Urteil des EGMR Michaud gegen Frankreich vom 6. Dezember 2012, 12323/11, §§ 96 f.; Urteil des EGMR Kennedy gegen Vereinigtes Königreich vom 18. Mai 2010, 26839/05, § 159; vgl. auch Urteil des EGMR Roman Zakharov gegen Russland vom 4. Dezember 2015, 47143/06, §§ 243–249 und Urteil des EGMR Amann gegen die Schweiz vom 16. Februar 2000, 27798/95, §§ 61 f.). Tragweite und Modalitäten der Massnahmen sind mithin unter Beachtung der Besonderheiten des Regelungsgegenstands so zu umschreiben, dass der Betroffene bei entsprechender Vorsicht und allenfalls mit juristischer Beratung sein Verhalten danach ausrichten und die Folgen seines Handelns entsprechend den Umständen vorhersehen kann (Urteil des EGMR Szabó und Vissy gegen Ungarn vom 12. Januar 2016, 37138/14, §§ 59 und 62). Es soll erkennbar sein, unter *welchen Umständen* und unter *welchen Bedingungen* der Staat ermächtigt ist, in die garantierten Rechte einzugreifen (Urteil des EGMR Malone gegen Vereinigtes Königreich vom 2. August 1984, 8691/79, § 67). Dabei ist es Aufgabe der nationalen Behörden und Gerichte, die innerstaatlichen, in Kraft stehenden Gesetze auszulegen und anzuwenden, wobei auch neue Entwicklungen in der Praxis zu berücksichtigen sind (zum Ganzen Urteil des EGMR Weber

und Saravia gegen Deutschland vom 29. Juni 2006, 54934/00, §§ 84, 90 und 92 ff.; Urteil des EGMR Malone gegen Vereinigtes Königreich vom 2. August 1984, 8691/79, §§ 67 f. und 79; BGE 138 I 6 E. 4.2 mit Hinweisen auf die Rechtsprechung des EGMR).

10.6

10.6.1 Im Streit liegt vorliegend die Pflicht der Anbieterinnen gemäss Art. 15 Abs. 3 BÜPF, die Randdaten der Telekommunikation der Beschwerdeführer zu speichern und während sechs Monaten aufzubewahren. Die Speicherung und Aufbewahrung der Randdaten lässt sich damit unumstritten auf eine formell-gesetzliche Grundlage stützen. Die Beschwerdeführer sind jedoch der Ansicht, die gesetzlich erfassten Tatbestände seien nicht hinreichend bestimmt formuliert und daher sei nicht vorhersehbar, welche Daten zu welchem Zweck gespeichert und aufbewahrt würden. Darauf ist im Folgenden vor dem Hintergrund des vorstehend Ausgeführten einzugehen.

10.6.2 Die Anbieterinnen sind nach Art. 15 Abs. 3 BÜPF verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren.

Die Begriffe "Teilnehmeridentifikation" sowie "Verkehrs- und Rechnungsdaten" sind technischer Natur und aus diesem Grund unbestimmt gehalten (vgl. www.duden.de etwa zum Wort "Verkehrsdaten"). Dies ist jedoch angesichts der Komplexität des Regelungsgegenstands, der Überwachung des Fernmeldeverkehrs, nicht grundsätzlich zu beanstanden, umso mehr, als die Bestimmung eine Verwaltungsmassnahme regelt und die privaten Anbieterinnen und nicht die Beschwerdeführer verpflichtet. Der Gesetzgeber kann, wie vorstehend erwogen, in dieser Materie nicht darauf verzichten, allgemeine und mehr oder minder vage Begriffe zu verwenden, deren Auslegung und Anwendung der Praxis überlassen werden muss. Allerdings dürfen auch nicht unnötig wesentliche Wertungen der Rechtsanwendung überlassen werden. Erforderlich ist ein den Umständen entsprechender bzw. optimaler Grad an Bestimmtheit, welcher es den Betroffenen ermöglicht, die freiheitsbeschränkenden Folgen ihres Handelns mit hinreichender Gewissheit vorauszusehen (BGE 109 Ia 273 E. 4d; vgl. zur jüngeren Rechtsprechung SCHWEIZER, a.a.O., Art. 36 Rz. 23; zudem HÄFELIN/MÜLLER/UHLMANN, a.a.O., Rz. 391 ff.). Dabei ist nicht allein auf den Wortlaut der betreffenden Bestimmung abzustellen. Vielmehr ist das Bestimmtheitserfordernis mit Blick auf die Umschreibung der umstrittenen Massnahme an Ziel und Zweck des Regelungsgegenstands zu messen und es ist nach

der Bedeutung zu fragen, die der Bestimmung im Kontext mit anderen Bestimmungen zukommt (vgl. BGE 139 II 243 E. 10, insbes. E. 10.1 f.; BGE 138 I 6 E. 5.3; BGE 136 I 87 E. 8.3; BGE 132 I 49 E. 6; ferner auch BGE 138 II 42 E. 4.2.1 und das Urteil des EGMR Leander gegen Schweden vom 26. März 1987, 9248/81, § 51).

Zu prüfen ist somit zunächst der Wortlaut von Art. 15 Abs. 3 BÜPF. Nach dem allgemeinen Sprachgebrauch meint *für die Teilnehmeridentifikation notwendigen Daten* alle Angaben, die notwendig sind, um die an einer Verbindung teilnehmenden Anschlüsse und (damit) die Teilnehmer einer fernmeldetechnischen Kommunikation zu bestimmen bzw. festzustellen (vgl. www.duden.de zum Wort "identifizieren"). Darunter fallen etwa Rufnummern und – soweit das Internet oder andere drahtlose und mobile Formen der Kommunikation genutzt werden – weitere Elemente wie IP-Adressen und Gerätenummern zur Identifikation der teilnehmenden Anschlüsse und damit der Teilnehmer. Eingeschlossen ist damit auch die IP-History, also Daten über den Internetverkehr einer Person wie etwa, wann im Internet gesurft und welcher Mailverkehr abgewickelt worden ist (vgl. HANSJAKOB, Bundesgerichtspraxis, S. 176 f.; wohl auch EMANUEL JAGGI, Die Revision des BÜPF, Schweizerische Zeitschrift für Strafrecht [ZStrR] 2015 S. 287 Fn. 71). Zudem werden die IP-Adressen der an einem Kommunikationsvorgang teilnehmenden Anschlüsse und nicht bloss diejenige des Ursprungs der Kommunikation gespeichert und aufbewahrt (vgl. Art. 24b Bst. a Ziff. 4 VÜPF, wonach die Übermittlung der verfügbaren Adressierungselemente, *insbesondere* des Ursprungs der Kommunikation, angeordnet werden kann). Hinzu kommen *Verkehrs- und Rechnungsdaten*. Darunter fallen nach dem allgemeinen Sprachgebrauch Angaben über die Kommunikation bzw. den Fernmeldeverkehr der Beschwerdeführer, welche von den Anbieterinnen etwa im Hinblick auf die Rechnungsstellung aufgezeichnet werden, also etwa Zeitpunkt und Dauer einer Verbindung. Die Anbieterinnen sind mithin verpflichtet, die mit dem Fernmeldeverkehr der Beschwerdeführer verbundenen Informationen zu speichern und aufzubewahren.

Eine wesentliche Einschränkung hinsichtlich dessen, was die Anbieterinnen gemäss Art. 15 Abs. 3 BÜPF zu speichern und aufzubewahren haben, ergibt sich aus dem Kontext mit Art. 15 Abs. 1 BÜPF, der folgenden Wortlaut aufweist:

> Art. 15 Pflichten der Anbieterinnen
>
> [1] Die Anbieterinnen von Fernmeldediensten sind verpflichtet, dem Dienst auf Verlangen den Fernmeldeverkehr der überwachten Person sowie die Teilnehmeridentifikation und Verkehrs- und Rechnungsdaten zuzuleiten. Ebenso haben sie die zur Vornahme der Überwachung notwendigen Informationen zu erteilen.
>
> …

Diese Bestimmung unterscheidet zwischen dem Inhalt des Fernmeldeverkehrs ("Fernmeldeverkehr der überwachten Person") und den mit dem Fernmeldeverkehr verbundenen Informationen bzw. den äusseren Daten des Kommunikationsvorgangs ("Teilnehmeridentifikation und Verkehrs- und Rechnungsdaten"). Die Bestimmung von Art. 15 Abs. 3 BÜPF erlaubt mithin keine Speicherung und Aufbewahrung von Kommunikationsinhalten. Was verbleibt, sind die äusseren Daten der Kommunikation, Daten also, aus denen etwa hervorgeht, mit wem die Beschwerdeführer wann und wie lange kommuniziert haben. Die Trennung von inhaltlicher Überwachung des Fernmeldeverkehrs und der (rückwirkenden) Erhebung von dessen äusseren Daten ergibt sich auch aus der Strafprozessordnung, die unterscheidet zwischen der Überwachung des Fernmeldeverkehrs (Art. 269 StPO) und der Auskunft über Verkehrs- und Rechnungsdaten sowie die Teilnehmeridentifikation (Art. 273 StPO).

10.6.3 Das BÜPF legt nach dem Gesagten den Zweck, die beteiligten Organe und das Ausmass der Datenbearbeitung jedenfalls in den Grundzügen selbst fest. Zwar sind die verwendeten Begriffe weniger bestimmt gehalten, doch lassen sich die Grundzüge der Regelung klar erkennen. Demnach sind die Anbieterinnen gemäss Art. 15 Abs. 3 BÜPF verpflichtet, die äusseren Daten der Telekommunikation im Hinblick auf eine Überwachung des Fernmeldeverkehrs zu speichern und während sechs Monaten aufzubewahren. Die Verpflichtung ist damit und mit Blick auf den Regelungsgegenstand in sachlicher wie auch in zeitlicher Hinsicht hinreichend bestimmt umschrieben und eingegrenzt; es werden keine wesentlichen Wertungen der Gesetzesanwendung überlassen.

Für die Beschwerdeführer ist somit gestützt auf Art. 15 Abs. 3 BÜPF vorhersehbar, dass die Anbieterinnen systematisch äussere Daten ihrer Kommunikation – in Abgrenzung zum Inhalt der Kommunikation – speichern und aufbewahren (vgl. in diesem Sinn BGE 138 I 6 E. 5.3; BGE 122 I 360 E. 5d; Urteil des EGMR Uzun gegen Deutschland vom 2. September 2010,

35623/05, § 68). Sie waren und sind somit in der Lage, die freiheitsbeschränkenden Folgen ihres Handelns – die Speicherung und Aufbewahrung von Daten als Folge der Nutzung von Kommunikationsdienstleistungen – mit hinreichender Gewissheit vorauszusehen. Hierfür ist es nicht notwendig, im Einzelnen zu wissen, welche (technischen) Daten gespeichert werden, sofern sich wie vorliegend das Ausmass der Datenbearbeitung in den Grundzügen aus dem Gesetz selbst ergibt (vgl. Urteil des EGMR Malone gegen Vereinigtes Königreich vom 2. August 1984, 8691/79, § 68). Vor diesem Hintergrund verfängt auch der Einwand der Beschwerdeführer nicht, dass für die Rechnungstellung je nach vertraglicher Beziehung zwischen den Beschwerdeführern und ihren jeweiligen Anbieterinnen kaum mehr detaillierte Angaben zu Zeitpunkt und Dauer der Verbindung notwendig sind. Auf die konkrete vertragliche Gestaltung der Beziehung zwischen den Beschwerdeführern und den Anbieterinnen kann es mit Blick darauf, dass letztere mit der Erfüllung einer öffentlichen Aufgabe betraut sind, nicht ankommen.

Auf der anderen Seite ist nicht ersichtlich, dass die Anbieterinnen Daten speichern und – im Rahmen etwa der Strafverfolgung – der Vorinstanz zuleiten würden, die nicht von Art. 15 Abs. 3 BÜPF erfasst sind; die Bestimmungen von Art. 16 Bst. d und Art. 24d VÜPF gehen hinsichtlich der Daten, deren Übermittlung angeordnet werden kann, nicht über Art. 15 Abs. 3 BÜPF hinaus. Dies gilt – unter dem Begriff der Verkehrsdaten – auch für (technische) Daten wie etwa den Standort und die Hauptstrahlrichtung der Antenne, mit der das Endgerät zum Zeitpunkt der Kommunikation verbunden ist (vgl. HANSJAKOB, Kommentar BÜPF, S. 88 f.). Hierzu kann auch auf die Materialien zum totalrevidierten BÜPF verwiesen werden. Demnach werden die Daten, welche gestützt auf Art. 15 Abs. 3 des geltenden Gesetzes gespeichert und aufbewahrt werden, neu wie folgt umschrieben (Art. 8 Bst. b des Entwurfs zu einem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BBl 2013 2789, 2791):

> Art. 8 Inhalt des Verarbeitungssystems
>
> Das Verarbeitungssystem enthält:
>
> …
>
> b. 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 (Randdaten des Fernmeldeverkehrs).
>
> …

Welche Daten von den Anbieterinnen zu speichern und aufzubewahren sind, wird somit unter dem Begriff "Randdaten" neu im Gesetz selbst umschrieben. Am materiellen Gehalt der Verpflichtung ändert sich nach den Materialien zum totalrevidierten BÜPF nichts (vgl. vorstehend E. 4.2.2). Somit ist davon auszugehen, dass auch das geltende Recht technische Merkmale der Verbindungen mit einschliesst und diese äusseren Daten von den Anbieterinnen gespeichert und aufbewahrt werden müssen (vgl. zum Ganzen und auch dazu, welche Informationen zur Vornahme der Überwachung zu erteilen sind, FAVRE, a.a.O., S. 86–95).

10.7 Die Rüge der ungenügenden Bestimmtheit von Art. 15 Abs. 3 BÜPF erweist sich damit – die Speicherung und den Umstand der Aufbewahrung betreffend – als unbegründet (zur Löschung der Daten und zu den [weiteren verfahrensrechtlichen] Garantien zum Schutz vor Missbrauch vgl. nachfolgend E. 12.7.4). In einem nächsten Schritt ist zu prüfen, ob sich die Einschränkung auf ein genügendes Eingriffsinteresse zu stützen vermag.

Eingriffsinteresse

11.

11.1 Einschränkungen von Grundrechten müssen durch ein öffentliches Interesse oder den Schutz von Grundrechten Dritter gerechtfertigt sein (Art. 36 Abs. 2 BV). Hierzu kann nicht jedes beliebige Interesse genügen. Einschränkungen können nur durch Interessen gerechtfertigt werden, die in der Rechtsordnung hinreichend Anerkennung gefunden haben. Allgemein anerkannte Eingriffsinteressen liegen insbesondere im Schutz von Polizeigütern und in der Erfüllung verfassungsrechtlich ausgewiesener Staatsaufgaben. Zudem geben Zwecknormen von Gesetzen und völkerrechtliche Normen Aufschluss über öffentliche Interessen, die Schutz verdienen (vgl. BGE 140 I 353 E. 8.6; BGE 136 I 87 E. 8.3; SCHWEIZER, a.a.O., Art. 36 Rz. 31 f. und 34; KIENER/KÄLIN, a.a.O., S. 115 f.; zudem BGE 138 I 378 E. 8.3). Dabei ist zu berücksichtigen, dass öffentliche Interessen wandelbar sind und einer politischen Wertung unterliegen (BGE 138 I 378 E. 8.3). Ob ein legitimes Eingriffsinteresse genügend Gewicht aufweist, um einen konkreten Grundrechtseingriff zu rechtfertigen, ist grundsätzlich im Rahmen der Verhältnismässigkeitsprüfung zu beurteilen (BGE 130 I 16 E. 5.2; EPINEY, a.a.O., Art. 36 Rz. 50; vgl. auch BGE 138 I 256 E. 5.5).

Auch nach Art. 8 Ziff. 2 EMRK darf eine Behörde in die Ausübung der in Ziff. 1 garantierten Rechte eingreifen. Voraussetzung ist, dass der Eingriff

gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Die Aufzählung ist abschliessend (KARPENSTEIN/MAYER, EMRK, Konvention zum Schutz der Menschenrechte und Grundfreiheiten, 2. Aufl. 2015, Art. 8 Rz. 96). Nach der Rechtsprechung reicht es nicht aus, wenn im konkreten Fall ein Interesse abstrakt betrachtet ein hinreichendes Motiv darstellt. Es ist auch zu prüfen, ob die konkret vorgesehenen Mittel innerhalb der Grenze dessen bleiben, was in einer demokratischen Gesellschaft tatsächlich notwendig ist (BGE 138 I 6 E. 4.3 und E. 5.5 f mit Hinweisen auf die Rechtsprechung des EGMR; hierzu nachfolgend E. 12).

11.2 Die Speicherung und Aufbewahrung von Randdaten i.S.v. Art. 15 Abs. 3 BÜPF ermöglicht eine rückwirkende Überwachung der Telekommunikation, welche nach Art. 1 Abs. 1 Bst. a BÜPF insbesondere ein Mittel der Strafverfolgung ist (vgl. vorstehend E. 2.2). Darüber hinaus dient sie der internationalen Rechtshilfe in Strafsachen sowie der Suche und Rettung vermisster Personen (Art. 1 Abs. 1 Bst. b und c BÜPF). An der Strafverfolgung und insbesondere auch an der Beweissicherung, welche die Speicherung und Aufbewahrung von Randdaten insbesondere ermöglichen soll, besteht unstrittig ein erhebliches öffentliches Interesse (BGE 128 II 259 E. 3.5; vgl. auch vorstehend E. 2.2 f.).

Auch im Kontext von Art. 8 Ziff. 2 EMRK kann mit Blick auf die Rechtsprechung des EGMR festgehalten werden, dass die Speicherung und Aufbewahrung von personenbezogenen Randdaten der Telekommunikation dem legitimen Ziel der Aufklärung von Straftaten dient; es soll eine Verbindung zwischen einer bestimmten Person und einer Straftat hergestellt werden (vgl. Urteil des EGMR Peruzzo und Martens gegen Deutschland vom 4. Juni 2013, 7841/08 und 57900/12, § 40; Urteil des EGMR Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, § 48). Die Regelung von Art. 15 Abs. 3 BÜPF betreffend die Speicherung und Aufbewahrung von Randdaten vermag sich somit auf ein hinreichendes Eingriffsinteresse zu stützen.

Verhältnismässigkeit

12.

12.1 Im Folgenden ist zu prüfen, ob die Speicherung und (zeitlich beschränkte) Aufbewahrung der Randdaten der Beschwerdeführer verhältnismässig ist bzw. im Rahmen dessen blieben, was in einer demokratischen Gesellschaft notwendig ist. Diese Prüfung hat sich, entsprechend der Trennung der verwaltungsrechtlichen von den strafprozessualen Aspekten der Überwachung des Fernmeldeverkehrs, auf die verwaltungsrechtliche Pflicht zur Speicherung und Aufbewahrung von Randdaten der Telekommunikation zu beschränken; die Frage, ob die Voraussetzungen für eine (rückwirkende) Überwachung gegeben sind und damit auch, ob eine konkrete Überwachungsanordnung verhältnismässig ist, ist im Rahmen einer Strafuntersuchung nach strafprozessualen Gesichtspunkten zu beurteilen (vgl. vorstehend E. 8.2). Zu beachten ist jedoch, dass die Speicherung nicht Selbstzweck ist, sondern im Hinblick auf die rückwirkende Überwachung des Fernmeldeverkehrs insbesondere zum Zweck der Strafverfolgung erfolgt. Die Verhältnismässigkeit der streitbetroffenen Massnahme wird anhand dieses Zwecks zu beurteilen sein, ohne dass sich damit jedoch etwas an der Trennung der verwaltungsrechtlichen von den strafprozessualen Aspekten der Überwachung des Fernmeldeverkehrs ändern würde.

12.2 Die Beschwerdeführer bringen vor, die Speicherung und Aufbewahrung von Randdaten – und damit auch die rückwirkende Überwachung des Fernmeldeverkehrs, wie ihn das BÜPF ermöglicht – sei unverhältnismässig. Die Massnahme sei nicht geeignet, effektiv einen Beitrag zur Strafverfolgung zu leisten und es bestünden andere Möglichkeiten, eine (rückwirkende) Überwachung zu ermöglichen; die Beschwerdeführer fordern, die Speicherung von Randdaten der Telekommunikation sei in zeitlicher und personeller Hinsicht zu beschränken, etwa indem Randdaten erst bei aufkommendem dringendem Tatverdacht gesichert würden (sog. quick freeze). Ihrer Ansicht nach fehlt es zudem an hinreichend bestimmten Regeln zur Gewährleistung der Datensicherheit, zur Löschung der Randdaten nach Ablauf der Aufbewahrungsfrist und zu wirksamen Kontroll- und Beschwerdemöglichkeiten, weshalb die Massnahme nicht zumutbar sei.

12.3 Einschränkungen von Grundrechten müssen verhältnismässig sein (Art. 36 Abs. 3 BV). Der Grundsatz der Verhältnismässigkeit verlangt, dass eine Massnahme für das Erreichen des im öffentlichen oder privaten Inte-

resse liegenden Ziels geeignet und erforderlich ist und sich für die Betroffenen in Anbetracht der Schwere der Grundrechtsverletzung zumutbar erweist. Die Verhältnismässigkeit misst sich am Verhältnis des Grundrechtseingriffs zum Zweck der Regelung, der dem öffentlichen Interesse bzw. dem Schutz der Grundrechte Dritter dienen muss (BGE 140 I 353 E. 8.7).

Konkret ist zu prüfen, ob das eingesetzte Mittel *geeignet* ist, den angestrebten Zweck zu erreichen oder zur Erreichung dieses Zwecks beizutragen; das öffentliche Interesse muss durch das staatliche Handeln wahrgenommen werden. Das eingesetzte Mittel muss zudem *erforderlich* sein, um den angestrebten Zweck zu erreichen; eine Einschränkung darf in sachlicher, räumlicher, zeitlicher und personeller Hinsicht nicht über das Notwendige hinausgehen. Es darf keine mildere, das Grundrecht weniger stark einschränkende Massnahme geben, mit der der angestrebte Zweck ebenso gut erreicht werden kann und die Massnahme darf – insbesondere nach der allgemeinen Lebenserfahrung – von ihrem räumlich-örtlichen Geltungsbereich nicht weiter gehen und nicht länger dauern, als notwendig. Eingriffe, die eine Vielzahl von Menschen treffen, sind sodann in personeller Hinsicht nur erforderlich, wenn der angestrebte Zweck nicht durch individuelle Anordnungen erreicht werden kann (EPINEY, a.a.O., Art. 36 Rz. 58; vgl. hinsichtlich der Beurteilung gestützt auf die allgemeine Lebenserfahrung etwa BGE 133 I 77 E. 5.2 f., BGE 130 I 16 E. 5.3; BGE 117 Ia 472 E. 3g sowie Urteil des BGer 1C_673/2013 vom 7. März 2014 E. 6.4). Der Grundsatz der Verhältnismässigkeit gebietet schliesslich eine Gewichtung und Abwägung der berührten Interessen. Erforderlich ist ein vernünftiges Verhältnis zwischen dem angestrebten Zweck und den gefährdeten privaten Interessen bzw. dem Interesse des Betroffenen an der Integrität seiner Grundrechte; die in Frage stehende Massnahme muss *zumutbar* sein. Es geht darum, einen Ausgleich zu finden zwischen – vorliegend – dem Recht auf Vertraulichkeit der Telekommunikation sowie der informationellen Selbstbestimmung und der Notwendigkeit, die (nachträgliche) Überwachung der Telekommunikation im Interesse der Strafverfolgung zu ermöglichen. Das öffentliche Interesse und die zum Schutz dieses Interesses gewählte Freiheitseinschränkung sollen in einem vernünftigen Verhältnis zueinander stehen (BGE 140 I 381 E. 4.5.1; vgl. auch BGE 127 I 164 E. 3b).

12.4 Vergleichbar führt die EMRK das Verhältnismässigkeitsprinzip in die Prüfung ein, indem sie die Zulässigkeit eines Eingriffs an das Kriterium der Notwendigkeit ("in einer demokratischen Gesellschaft notwendig") einer Massnahme knüpft. Dabei berücksichtigt der EGMR die wesentlichen Merkmale einer demokratischen Gesellschaft ("pluralisme, tolérance et

esprit d'ouverture"; Urteil des EGMR Chassagnou und Andere gegen Frankreich vom 29. April 1999, 25088/94, 28331/95 und 28443/95, § 112). Er zieht zudem – wenn auch nicht ausdrücklich – die Kriterien der Erforderlichkeit, Geeignetheit und Angemessenheit bei (KARPENSTEIN/MAYER, a.a.O., Art. 8 Rz. 97).

In seiner Rechtsprechung zu Art. 8 EMRK hebt der EGMR die Bedeutung des Schutzes personenbezogener Daten für die in Art. 8 Ziff. 1 EMRK garantierten Rechte hervor und betont – insbesondere mit Blick auf die Gefahr einer missbräuchlichen Verwendung gerade elektronischer Daten auch durch Private – die Notwendigkeit einer wirksamen Missbrauchskontrolle. Betroffene müssten wirksame und effektive Möglichkeiten der Kontrolle von Eingriffen in ihr Recht auf Korrespondenz und (damit) ihr Recht auf Schutz personenbezogener Daten haben (Urteil des EGMR Peruzzo und Martens gegen Deutschland vom 4. Juni 2013, 7841/08 und 57900/12, § 42; Urteil des EGMR S. und Marper gegen Vereinigtes Königreich vom 4. Dezember 2008, 30562/04 und 30566/04, § 103; Urteil des EGMR Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, § 49 ff.; vgl. auch BGE 138 I 6 E. 4.3 mit Hinweisen auf die Rechtsprechung des EGMR). Bei der Beurteilung der Verhältnismässigkeit ist ferner der Art der Daten und ihrer Bedeutung für den Kernbereich der Persönlichkeit des Betroffenen angemessen Rechnung zu tragen (GRABENWARTER/PABEL, a.a.O., § 22 Rz. 45).

12.5 Das Bundesgericht hat im Zusammenhang mit der (rein strafprozessualen) Überprüfung von Überwachungsmassnahmen wiederholt festgehalten, dass das Resultat einer rückwirkenden Randdatenerhebung für die Aufklärung und die rechtliche Qualifikation des untersuchten Delikts von wesentlicher Bedeutung sein könne. So kann nach der Rechtsprechung die rückwirkende Überwachung geeignet sein, das Tatmotiv eines Beschuldigten und die genauen Umstände der Tat zu eruieren und es können Informationen zum persönlichen Verhältnis zwischen Opfer und Beschuldigtem sowie zu den Beziehungsnetzen erhältlich gemacht werden (Urteil des BGer 1B_251/2013 vom 30. August 2013 E. 3 und 5.5). Im Zusammenhang mit einer Strafuntersuchung wegen banden- und gewerbsmässigen Diebstahls, Sachbeschädigung und Hausfriedensbruchs dienten die Randdatenerhebungen und entsprechende Abgleichungen namentlich dem Zweck, zu prüfen, ob sich die Beschuldigten zu den Zeitpunkten und an den Tatorten weiterer einschlägiger Delikte untereinander oder mit anderen Personen telefonisch verabredet hatten (Untersuchung sowohl entals auch belastender Indizien; vgl. Urteil des BGer 1B_365/2014 vom

12. Januar 2015 E. 6.4; vgl. auch das Urteil des BGer 1B_59/2014 vom 28. Juli 2014 E. 4.4 und hinsichtlich der Identifikation von Mittätern HANSJAKOB, Kommentar BÜPF / VÜPF, S. 109). In einem anderen Fall sollte der Abgleich von Verbindungsranddaten der Abklärung dienen, ob mehrere Raubüberfälle zumindest teilweise von derselben Täterschaft ausgeführt wurden; das Bundesgericht erachtete in diesem Zusammenhang Antennensuchläufe unter bestimmten Voraussetzungen für zulässig (BGE 137 IV 340 E. 5 und 6).

Es kann somit nicht in Abrede gestellt werden, dass die Speicherung und Aufbewahrung von Randdaten und damit die rückwirkende Überwachung des Fernmeldeverkehrs geeignet ist, zur Aufklärung von Straftaten beizutragen. Dies gilt umso mehr, als mit der rückwirkenden Überwachung nicht erst die nach Vorliegen eines begründeten Verdachts, sondern schon in einem früheren Stadium angefallenen Daten erhältlich gemacht werden können (vgl. WEBER/WOLF/HEINRICH, Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung, Jusletter vom 12. März 2012, S. 2; Botschaft BÜPF, BBl 1998 IV 4241, 4259, wonach die Randdaten für die Strafverfolgung deshalb von zunehmender Bedeutung sind, weil sie auch Informationen über den in der Vergangenheit geführten Fernmeldeverkehr ermöglichen; zudem HANSJAKOB, Kommentar BÜPF / VÜPF, S. 150;). Die vorstehend in zusammenfassender Weise wiedergegebenen Erwägungen des Bundesgerichts zur Eignung der rückwirkenden Überwachung können zudem und entgegen der Ansicht der Beschwerdeführer durchaus in einem gewissen Masse verallgemeinert werden. Der Verhältnismässigkeitsgrundsatz verlangt aus Sicht des Grundrechtsschutzes schliesslich nicht, dass die Erhebung von Randdaten in jedem Fall von unmittelbarer Bedeutung für die Aufklärung einer Straftat sein muss. An das Subsidiaritätsprinzip, welches das Verhältnismässigkeitsprinzip konkretisiert, sind insbesondere beim Verdacht eines schweren Verbrechens grundsätzlich keine allzu hohen Anforderungen zu stellen (Urteil des BGer 1B_265/2012 vom 21. August 2012 E. 2.3; vgl. in diesem Sinne auch das Urteil des Verfassungsgerichtshofs Österreich vom 27. Juni 2014, G 47/2012-49, E. 2.3.10 und E. 2.3.14.1, abrufbar unter < www.vfgh.gv.at > Rechtsprechung > Ausgewählte Entscheidungen > 2014 [besucht am 25. Oktober 2016]). Vielmehr reicht es aus, wenn die Überwachungsmassnahme darauf abzielt, eine unverhältnismässige Erschwerung komplexer Untersuchungen zu vermeiden (Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 Bst. c StPO; Urteil des BGer 1B_365/2014 vom 12. Januar 2015 E. 6.4). Es rechtfertigt sich daher und auch mit Blick auf

die vorstehend zitierte Rechtsprechung nicht, der rückwirkenden Überwachung des Fernmeldeverkehrs generell die Eignung abzusprechen. Zudem ermöglicht die Speicherung und Aufbewahrung der Randdaten eine differenzierte rückwirkende Überwachung, indem den Strafverfolgungsbehörden ermöglicht wird, anhand verschiedener Targets, d.h. anhand verschiedener technischer Parameter wie etwa der Rufnummer eines Verdächtigen oder der Gerätenummer eines von ihm benutzten Geräts, einen bestimmten Fernmeldeverkehr zu überwachen (vgl. HANSJAKOB, Bundesgerichtspraxis, S. 174 und S. 176; ferner das Urteil des deutschen Bundesverfassungsgerichts 1 BvR 256/08 vom 2. März 2010 Rz. 207, abrufbar unter < www.bundesverfassungsgericht.de > Entscheidungen > vor 2012 > 2010 > März [besucht am 25. Oktober 2016]). Der Verfahrensantrag de Beschwerdeführer, es sei die Praxis im Zusammenhang mit der Anordnung von Massnahmen zur rückwirkenden Überwachung des Fernmeldeverkehrs sowie deren richterlicher Überprüfung zu evaluieren, ist somit in vorwegnehmender Beweiswürdigung abzuweisen, sofern er sich überhaupt als zulässig erweist.

An diesem Ergebnis ändert (für sich alleine) nichts, dass das Max-Planck-Institut 2011 zu dem Ergebnis gekommen ist, es liessen sich keine Hinweise darauf finden, dass die in der Schweiz seit mehreren Jahren praktizierte Speicherung und Aufbewahrung von Randdaten zu einer systematisch höheren Aufklärung von Straftaten geführt hätte. So ist in der Studie denn auch festgehalten, es bestünden erst unsichere Datengrundlagen, systematische empirische Untersuchungen fehlten weitgehend und die befragten Praktiker würden sich teilweise widersprechen (Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Juli 2011, S. 83, 129 f., 188 und 218 ff., abrufbar unter < www.mpicc.de > Forschung > Forschung im Detail > Kriminologische Abteilung > Strafverfahren und Sanktionen im Wandel [besucht am 25. Oktober 2016]; vgl. auch die Anmerkung in NICOLE BERANEK ZANON, Datenaufbewahrungspflichten vs. Datenlöschungspflichten, Kollision von BÜPF und DSG, in: Weber/Thouvenin [Hrsg.], Neuer Regulierungsschub im Datenschutzrecht?, 2012, S. 154).

12.6 Die Beschwerdeführer wenden weiter ein, die anlasslose Speicherung und Aufbewahrung von Randdaten der Kommunikation gehe in sachlicher, zeitlicher und personeller Hinsicht über das Notwendige hinaus. Sie fordern, Randdaten sollten erst bei aufkommendem dringendem Tatver-

dacht auf Anordnung der Strafverfolgungsbehörden vorübergehend gespeichert und auf richterlichen Beschluss hin zugänglich gemacht werden. Die Speicherung und Aufbewahrung von Randdaten würde damit auf jene Daten beschränkt, die in engem zeitlichem, örtlichem und sachlichem Zusammenhang mit der zu untersuchenden Straftat angefallen sind.

Diese Massnahme des sog. quick freeze erscheint jedoch nicht gleich effektiv und damit nicht gleich wie die anlasslose Speicherung und (zeitlich beschränkte) Aufbewahrung von Randdaten i.S.v. Art. 15 Abs. 3 BÜPF geeignet, zur Strafverfolgung beizutragen. Sie käme vielmehr einer Echtzeit-Überwachung nahe. Jedenfalls würde eine rückwirkende Überwachung praktisch verunmöglicht, da Randdaten erst nach Aufkommen eines begründeten dringenden Verdachts erhältlich gemacht werden könnten. Der vom Gesetzgeber geschaffenen und gewollten Möglichkeit der rückwirkenden Überwachung ist es immanent, dass (Rand-)Daten anlasslos gespeichert und (zeitlich begrenzt) aufbewahrt werden. Oder mit anderen Worten ausgedrückt: Eine rückwirkende Überwachung ist nur möglich, wenn Randdaten anlasslos gespeichert und während einer bestimmten Zeit aufbewahrt werden. Im Weiteren bleibt unklar, was die Beschwerdeführer – im Unterschied zur Echtzeit-Überwachung – unter "*aufkommendem* dringendem Tatverdacht" verstehen. Der Zugang zu Informationen über den in der Vergangenheit geführten Fernmeldeverkehr und damit eine Sicherung entsprechender Beweise würde mit der von den Beschwerdeführern vorgeschlagenen Massnahme jedenfalls verunmöglicht. Dies träfe offenkundig insbesondere die Verfolgung jener Straftaten nachteilig, deren Entdeckung nicht sogleich erfolgt oder wenn bei einem Antragsdelikt der Antrag erst gegen Ende der Antragsfrist von drei Monaten gestellt wird (Art. 31 StGB). Anzumerken ist in diesem Zusammenhang, dass der Gesetzgeber anlässlich der Totalrevision des BÜPF die Einführung des quick freeze ausdrücklich abgelehnt hat (AB 2015 N 1165, dritte Abstimmung zum Antrag der Minderheit IV; vgl. auch die Voten von Bundespräsidentin Simonetta Sommaruga, AB 2015 N 1160 und von Jean Christophe Schwaab für die Kommission, AB 2015 N 1161). Die streitbetroffene Verpflichtung i.S.v. Art. 15 Abs. 3 BÜPF geht somit in personeller und auch in zeitlicher Hinsicht nicht über das hinaus, was zur Zielerreichung notwendig ist (kritisch zur Notwendigkeit KOLB, a.a.O., S. 118 f.). Zum Zweck der Strafverfolgung ist vielmehr eine gewisse Aufbewahrungsdauer notwendig (vgl. BGE 139 IV 98 E. 4.6), wobei die parlamentarischen Beratungen im Zusammenhang mit der Totalrevision des BÜPF zeigen, dass die Aufbewahrung der Randdaten über ein halbes Jahr mit Blick auf die Strafverfolgung an der unteren Grenze des

Erforderlichen angesetzt ist (vgl. Botschaft nBÜPF, BBl 2013 2683, 2741; Votum Bundesrätin Simonetta Sommaruga, AB 2016 N 134).

Die Speicherung einer Vielzahl von Randdaten ermöglicht es den Strafverfolgungsbehörden sodann – wie bereits erwähnt – eine differenzierte rückwirkende Überwachung anhand verschiedener Targets. Würden – wie von den Beschwerdeführern gefordert – weniger Daten gespeichert, so könnte u.U. eine rückwirkende Überwachung nicht durchgeführt werden, weil Daten für eine Anknüpfung fehlen. Für eine rückwirkende Überwachung ist es daher erforderlich, möglichst eine Vielzahl verschiedener Randdaten zu speichern, wobei daraus nicht geschlossen werden darf, Randdaten seien schrankenlos zu speichern. Vorliegend ist jedoch nicht ersichtlich, dass die zu speichernden und aufzubewahrenden Randdaten in sachlicher Hinsicht über das hinausgehen, was zur Erreichung des Zwecks notwendig ist. In diesem Zusammenhang ist auch darauf hinzuweisen, dass nach der geltenden gesetzlichen Ordnung die Randdaten zwar anlasslos gespeichert, den Strafverfolgungsbehörden jedoch erst bei dringendem Tatversacht und unter Beachtung des Verhältnismässigkeitsgrundsatzes zugeleitet werden dürfen (Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 Bst. a und c StPO).

12.7

12.7.1 Die Beschwerdeführer kritisieren die streitbetroffene Speicherung und Aufbewahrung von Randdaten ihrer Telekommunikation schliesslich als unzumutbar. Sie sehen die streitbetroffene Massnahme im Widerspruch zu den Anforderungen des Datenschutzes bzw. zu verschiedenen datenschutzrechtlichen Grundsätzen stehen. Konkret fehle es an griffigen Vorschriften zur Datensicherheit – etwa dazu, wer seitens der Anbieterinnen Zugriff auf die Daten habe und wo diese zu speichern seien – und zur Löschung der gespeicherten Randdaten; eine Löschung der Daten nach Ablauf der gesetzlichen Aufbewahrungsdauer sei gesetzlich nicht vorgeschrieben. Zudem sei den Beschwerdeführern seitens der Anbieterinnen nicht umfassend Einsicht in die über sie gespeicherten Daten gewährt worden. Vor diesem Hintergrund erschienen ihre grundrechtlich geschützten Positionen, das Recht auf Vertraulichkeit ihrer Kommunikation sowie auf informationelle Selbstbestimmung, als gewichtiger als das Interesse, die nachträgliche Überwachung im Interesse der Strafverfolgung zu ermöglichen. Demgegenüber hält die Vorinstanz die gesetzlich vorgesehenen Vorkehren gegen einen Missbrauch der gespeicherten Daten für zureichend, wobei sie in allgemeiner Weise auf die strafprozessualen Bestimmungen und die Datenschutzgesetzgebung verweist.

12.7.2 Das Bundesgericht wie auch der EGMR haben sich im Zusammenhang mit (geheimen) Überwachungsmassnahmen und im Rahmen abstrakter Normenkontrollen bereits verschiedentlich zur Bearbeitung und damit zur Aufbewahrung von Personendaten geäussert. Darauf ist im Folgenden vorab einzugehen. Anschliessend wird geprüft, ob das geltende Recht diesen Anforderungen genügt (nachfolgend E. 12.7.3 f.) und es werden die sich gegenüberstehenden Interessen gegeneinander abzuwägen sein (nachfolgend E. 12.8).

Der EGMR betont in konstanter Rechtsprechung, aus der Überwachung resultierende Eingriffe in grund- und konventionsrechtlich geschützte Positionen könnten nur dann als notwendig angesehen werden, wenn die gesetzliche Ordnung ausreichende Garantien zum Schutz vor Missbrauch vorsehe (Urteil des EGMR Malone gegen Vereinigtes Königreich vom 2. August 1984, 8691/79, § 81). Er verlangt entsprechend, dass die Art der Daten, die aufgezeichnet werden können, die Umstände, unter denen Überwachungsmassnahmen angeordnet werden dürfen, die Vorsichtsmassnahmen im Umgang mit aufgezeichneten Daten, die Zeitdauer der Aufbewahrung und das Verfahren für die Auswertung, Verwendung und Speicherung einschliesslich der Kreis der zugriffsberechtigten Personen und der Löschung der Daten im Gesetz selbst umschrieben sind (Urteil des EGMR Association for European Integration and Human Rights and Ekimdzhiev gegen Bulgarien vom 28. Juni 2007, 62540/00, §§ 75–77; Urteil des EGMR Weber und Saravia gegen Deutschland vom 29. Juni 2006, 54934/00, §§ 95–101; Urteil des EGMR Rotaru gegen Rumänien vom 4. Mai 2000, 28341/95, § 57 f.; vgl. auch vorstehend E. 10.5 und die zusammenfassende Darstellung bei WEBER/SOMMERHALDER, a.a.O., S. 95).

Entsprechende Anforderungen an die gesetzliche Grundlage im Zusammenhang mit der Überwachung der Telekommunikation und der Bearbeitung personenbezogener Daten ergeben sich auch aus der Rechtsprechung des Bundesgerichts, so etwa aus BGE 133 I 77 betreffend die im Polizeireglement der Stadt St. Gallen vorgesehene Aufbewahrung von Videomaterial aus der Überwachung öffentlicher Plätze. Das Bundesgericht erachtete die im Polizeireglement vorgesehene *Aufbewahrungsdauer* von 100 Tagen als verhältnismässig. Viele Strafuntersuchungen würden erst auf Anzeige oder Strafantrag hin eingeleitet, wobei Betroffene damit insbesondere aus persönlichen Gründen oft zuwarteten. Eine gewisse Aufbewahrungsdauer sei daher erforderlich, damit die Aufzeichnungen eine effektive Strafverfolgung überhaupt ermöglichen könnten; bei Straftaten auf

öffentlichem Grund seien solche Aufzeichnungen häufig das einzig aussagekräftige Beweismaterial (BGE 133 I 77, E. 5). Eine Aufbewahrungsdauer von einem Jahr erachtete das Bundesgericht hingegen als unverhältnismässig, da in einem solchen Fall insbesondere die Gefahr einer missbräuchlichen Verwendung der Aufzeichnungen verstärkt ins Gewicht falle (BGE 136 I 87 E. 8.4; vgl. auch BGE 133 I 77 E. 5.3; zudem das Urteil des EGMR Peruzzo und Martens gegen Deutschland vom 4. Juni 2013, 7841/08 und 57900/12, § 46).

Im Zusammenhang mit der Beurteilung des Polizeireglements der Stadt St. Gallen hielt das Bundesgericht zudem fest, dass sich die Verhältnismässigkeit der streitigen Massnahme, nämlich der Aufbewahrung von Überwachungsmaterial, nicht allein nach deren Dauer bestimme. Mit in die Beurteilung einzubeziehen sei auch, wie und von wem dieses verwendet werde und in welchem Ausmass die Personen, deren Daten aufgezeichnet seien, vor einem nicht sachgerechten Zugriff auf die Aufzeichnungen und einer missbräuchlichen Verwendung der Daten geschützt seien. Dem Polizeireglement lasse sich jedoch keine hinreichende Regelung der *Zugriffsberechtigung* entnehmen und es bleibe unklar, wie die Daten *vor unbefugter Kenntnisnahme, Bearbeitung und Entwendung zu sichern* seien. Zudem sei offen, mit welcher Unabhängigkeit und mit welchen Kompetenzen das zuständige *Datenschutzorgan* den Schutz der Aufzeichnungen vor unsachgemässer Verwendung tatsächlich wahrnehmen könne (BGE 133 I 77 E. 5.4). Den weiteren Erwägungen ist sodann Folgendes zu entnehmen (BGE 133 I 77 E. 5.4 f.):

> Im Interesse von Rechtssicherheit und Rechtsklarheit wäre eine Regelung im Polizeireglement angezeigt gewesen. Es ist indes davon auszugehen, dass die Stadt St. Gallen die kantonalen und auch für die Gemeinde geltenden Vorschriften über den Datenschutz beachtet. Entsprechende Garantien sind insbesondere im Staatsverwaltungsgesetz […] und in der Datenschutzverordnung […] enthalten.
>
> […] Darüber hinaus ist der Stadtrat darauf zu behaften, nach Art. 3 Abs. 4 des Polizeireglements mit wirksamen Vorkehrungen sicherzustellen, dass jegliche missbräuchliche Verwendung des Aufzeichnungsmaterials ausgeschlossen wird. Im Rahmen der abstrakten Normenkontrolle ist am Vollzug dieser gesetzlichen Auflagen nicht zu zweifeln. Unter diesen Umständen kann eine verfassungs- und EMRK-konforme Anwendung der Aufbewahrungsdauer von 100 Tagen […] angenommen werden.

In ähnlicher Weise hat sich das Bundesgericht in BGE 137 I 167 im Zusammenhang mit dem Gesetz des Kantons Genf über die Prostitution geäussert, das eine Meldepflicht für sich prostituierende Personen gegenüber

der Polizei vorsah. Zwar würde das kantonale Gesetz die Speicherung, den Schutz und den künftigen Gebrauch der zu speichernden Personendaten nicht (ausdrücklich) regeln. Unter Berücksichtigung des vom DSG und dem kantonalen Recht in diesem Bereich festgesetzten klaren Rahmens genüge indessen der globale Verweis auf die Gesetzgebung im Bereich des Persönlichkeits- und Datenschutzes im Rahmen der abstrakten Normenkontrolle (BGE 137 I 167 E. 9.1).

Im Zusammenhang mit der Aufbewahrung von Personendaten in einem polizeilichen Informationssystem anerkannte das Bundesgericht sodann das Recht betroffener Personen, sich gestützt auf das informationelle Selbstbestimmungsrecht dagegen zur Wehr zu setzen, dass ihre Personendaten ohne ersichtlichen Grund auf lange Zeit in einem öffentlichen Register gespeichert würden. Wann dies im Einzelfall zutreffe, hänge im Wesentlichen von den konkreten Umständen ab. Das Bundesgericht ging mit Blick auf den Zweck der Datenaufbewahrung davon aus, diese liege im öffentlichen Interesse an der Verfolgung einer unaufgeklärten Straftat und (damit) auch im Interesse von Opfern und Geschädigten; es bestehe die Möglichkeit, über bestimmte Daten dank der Datenvernetzung des Informationssystems auf weitere Daten zu stossen, die zusammen mit neuen Erkenntnissen die Ermittlungsarbeiten voranbringen könnten. In diesem Fall sei eine Interessenabwägung vorzunehmen, wobei insbesondere der Kreis der zum Informationssystem *Zugangsberechtigten* mit in die Abwägung einzubeziehen sei (BGE 138 I 256 E. 5.3 und 5.5; vgl. zudem BGE 107 Ia 148 E. 2).

Das Bundesgericht und der EGMR verlangen sodann, dass die *Löschung bzw. Vernichtung der gespeicherten Daten* verbindlich geregelt ist (vgl. vorstehend E. 10.4 f.). In BGE 136 I 87 war u.a. die Bestimmung in einem kantonalen Polizeigesetz zu beurteilen, wonach Aufzeichnungen aus Überwachungen zu löschen seien, wenn feststehe, dass sie nicht mehr benötigt würden. Nach den Erwägungen des Bundesgerichts ist eine solche Bestimmung zu unbestimmt, um eine echte Begrenzung darzustellen; es sei nicht ersichtlich, welche Zweckrichtung der Benötigung zukomme und ob die Formulierung "wenn feststeht" einen formellen Entscheid voraussetze (BGE 136 I 87 E. 8.4). Im Zusammenhang mit der Erstellung von DNA-Identifizierungsmustern erachtete der EGMR sodann eine gesetzliche Regelung, welche zwar keine Fristen vorgab, jedoch vorsah, dass die zuständige Behörde periodisch prüft, ob die fortdauernde Speicherung noch erforderlich ist, und die Daten – es ging um DNA-Identifizierungsmuster – spätestens nach zehn Jahren zu löschen sind, als verhältnismässig (Urteil

des EGMR Peruzzo und Martens gegen Deutschland vom 4. Juni 2013, 7841/08 und 57900/12, § 46).

Von einer Bearbeitung ihrer Daten betroffenen Personen muss schliesslich ein *Recht auf Auskunft und Einsicht* in die betreffenden Daten zukommen. Nach der Rechtsprechung des Bundesgerichts ist dies unentbehrliche Voraussetzung für die Verwirklichung des von der Verfassung garantierten Schutzes der Privatsphäre (BGE 138 I 6 E. 7.5.2; Frage, ob sich aus der Verfassung ein Recht auf Auskunft ergibt, offen gelassen in BGE 133 Ia 257 E. 4c f.). Damit einher geht – mit Blick auch auf Art. 13 EMRK – der Anspruch betroffener Personen auf eine wirksame *Kontroll- bzw. Beschwerdemöglichkeit*, spätestens nach dem Wegfall allfälliger Geheimhaltungsinteressen (BGE 138 I 6 E. 6.2 f.; vgl. auch Urteil des EGMR Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, §§ 50 und 55 ff.). So hielt der EGMR bereits früh im Zusammenhang mit der deutschen Gesetzgebung zur geheimen Telefonüberwachung mit Blick insbesondere auf die Entwicklung des Terrorismus fest, dass diese zum Schutz der nationalen Sicherheit sowie der öffentlichen Sicherheit und Ordnung in einer demokratischen Gesellschaft notwendig sei, soweit angemessene und wirkungsvolle Massnahmen zum Schutz vor Missbrauch – insbesondere vor einer falschen und missbräuchlichen Verwendung personenbezogener Daten – bestünden. Im konkreten Fall erachtete er die Kontrolle durch eine parlamentarische Kontrollkommission für ausreichend (Urteil des EGMR Klass und andere gegen Deutschland vom 6. September 1978, 5029/71, §§ 48 ff.).

12.7.3 Dem BÜPF lässt sich hinsichtlich des Umgangs mit personenbezogenen Daten bzw. zum Datenschutz unmittelbar nichts entnehmen. Und auch die Materialien bringen keine grundsätzliche Klärung. Immerhin hält der Bundesrat in seiner Botschaft fest, der Datenschutz gebiete es, gespeicherte Randdaten nach Ablauf der Aufbewahrungsdauer zu löschen (Botschaft BÜPF, BBl 1998 IV 4241, 4268). Während der parlamentarischen Beratung ist zudem festgehalten worden, dass die Vorinstanz der Aufsicht durch den Eidgenössischen Datenschutzbeauftragten nach Art. 27 DSG unterworfen sei (Votum Dorle Vallender für die Kommission, AB 1999 N 2613).

Die VÜPF enthält in Art. 7 ff. verschiedene Bestimmungen zur Bearbeitung von Personendaten sowie zum Datenschutz und zur Datensicherheit. Zunächst erlaubt Art. 7 Abs. 1 VÜPF die Bearbeitung jener Personendaten

durch die zuständigen Strafverfolgungsbehörden sowie durch die Anbieterinnen, die sie für die Kontrolle der Ausführung der Überwachungsanordnungen benötigen. Für die Gewährleistung der Datensicherheit gelten die Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11) und – für die Bundesverwaltung – die Bestimmungen der Bundesinformatikverordnung vom 9. Dezember 2011 (BinfV, SR 172.010.58; Art. 9 Abs. 1 VÜPF; Art. 1 BinfV). Die Anbieterinnen haben bezüglich der Übertragung der Überwachungsdaten sodann den Anweisungen der Vorinstanz zu folgen und sind bis zum Übergabepunkt der Daten an die Vorinstanz für die Datensicherheit verantwortlich (Art. 9 Abs. 2 VÜPF).

Aus dem Verweis auf die VDSG ergibt sich eine Klärung bezüglich der für die Anbieterinnen geltenden Anforderungen an die Datensicherheit bei der Bearbeitung von Personendaten. Zunächst ist jedoch zu klären, welchen Bestimmungen der VDSG die Anbieterinnen unterworfen sind, jenen für private Personen gemäss Art. 1 ff. VDSG oder jenen für Bundesorgane gemäss Art. 13 ff. VDSG.

Die Anbieterinnen sind als Private – soweit vorliegend von Interesse – mit einer öffentlichen Aufgabe des Bundes betraut und es steht den Anbieterinnen und den Beschwerdeführern nicht frei, Speicherung und Aufbewahrung von Randdaten sowie deren allfällige Herausgabe abweichend von den Bestimmungen des BÜPF zu regeln (vorstehend E. 2.3). Die Anbieterinnen gelten daher, soweit sie gestützt auf Art. 15 Abs. 3 BÜPF Randdaten der Telekommunikation speichern und aufbewahren, als Organe des Bundes (Art. 3 Bst. h DSG; vgl. auch BERANEK ZANON/DE LA CRUZ BÖHRINGER, a.a.O., Rz. 9.59, wonach die Beurteilung, ob es sich beim Datenbearbeiter um eine Privatperson oder um ein Bundesorgan handelt, von der rechtlichen Natur der Tätigkeit abhängt). Sie sind datenschutzrechtlich denjenigen Bestimmungen unterworfen, welche für die Bearbeitung von Personendaten durch Bundesorgane gelten (vgl. zum Ganzen MAURER-LAMBROU/KUNZ, in: Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, Art. 2 DSG Rz. 14; GABOR P. BLECHTA, in: Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, Art. 3 DSG Rz. 83 f.; PHILIPPE MEIER, Protection des données, 2011, Rz. 362, 365 und 600 ff.). Für die Anbieterinnen gelten entsprechend die Bestimmungen gemäss Art. 13 ff. VDSG, wobei jedoch Art. 20 Abs. 1 VDSG hinsichtlich der technischen und organisatorischen Massnahmen auf die Art. 8–10 VDSG zurückverweist; die verantwortlichen

Bundesorgane treffen 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 (Art. 20 Abs. 1 VDSG).

Nach Art. 8 Abs. 1 VDSG hat, wer Personendaten bearbeitet, für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten zu sorgen, um einen angemessenen Datenschutz zu gewährleisten. Verlangt ist kein absoluter Datenschutz bzw. kein absoluter Schutz der Daten vor unbefugtem Zugriff; es sind die im Einzelfall gestützt auf eine Risikoanalyse verhältnismässigen Massnahmen zu treffen (CHRISTA STAMM-PFISTER, in: Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, Art. 7 DSG Rz. 9). In Art. 8 Abs. 2 VDSG sind in nicht abschliessender Weise die bei der Wahl der Massnahmen zu beachtenden Kriterien genannt, wobei an dieser Stelle festgehalten werden kann, dass besonders schützenswerte Personendaten wie vorliegend die Randdaten der Telekommunikation (vgl. vorstehend E. 9.4) einen erhöhten Schutz benötigen (ASTRID EPINEY, in: Belser/Epiney/Waldmann [Hrsg.], Datenschutzrecht, 2011, § 9 Rz. 53). Bei der Pflicht, die angemessenen Massnahmen zum Schutz von Personendaten zu ergreifen, handelt es sich um eine Dauerpflicht und die getroffenen Massnahmen sind zudem periodisch zu überprüfen (Art. 8 Abs. 3 VDSG; BVGE 2012/14 E. 9.1). Als Massnahmen kommen solche technischer und organisatorischer Natur in Betracht, also etwa IT-Sicherheitsmassnahmen (beispielsweise Datenverschlüsselung, Passwortschutz, Firewalls, Protokollierung von Datenzugriffen) oder das Einschränken der Zugriffsberechtigung im Rahmen eines Zugriffskonzepts (BERANEK ZANON/DE LA CRUZ BÖHRINGER, a.a.O., Rz. 9.94). Personendaten sollen intern gesetzeskonform bearbeitet und gegen aussen hin vor einem unbefugten Zugriff durch Dritte geschützt werden. Die Bestimmungen von Art. 8–10 VDSG enthalten Präzisierungen der zu ergreifenden Massnahmen, insbesondere wenn Personendaten automatisiert bearbeitet werden (vgl. hierzu die Kritik von BRUNO BAERISWYL, in: Baeriswyl/Pärli, Datenschutzgesetz [DSG], 2015, Art. 7 Rz. 15). Mit Blick auf Zweck und Umfang der Datenbearbeitung scheint es vorliegend gerechtfertigt, von den Anbieterinnen grundsätzlich die Erarbeitung eines umfassenden Sicherheits- bzw. Datenschutzkonzepts zu verlangen, in welchem etwa anhand internationaler Standards insbesondere die Schutzziele definiert, die Risiken analysiert und die organisatorischen und technischen Massnahmen umschrieben sowie Verantwortlichkeiten zugewiesen werden (BAERISWYL, a.a.O., Art. 7 Rz. 38 f.); die Implementierung isolierter Einzelmassnahmen erscheint für die Sicherstellung der Datensicherheit nicht ausreichend

(STAMM-PFISTER, a.a.O., Art. 7 DSG Rz. 12). Ein solches Konzept ermöglicht bzw. erleichtert die spezifische Aufsicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemäss Art. 27 DSG (YVONNE JÖHRI, Aufgaben und Bedeutung der öffentlichen Datenschutzbeauftragten, in: Passadelis/Rosenthal/Thür, Datenschutzrecht, 2015, Rz. 8.32 und 8.39 [betreffend die Kompetenzen des EDÖB]; vgl. auch nachfolgend E. 12.7.5). Das Sicherheitskonzept ist periodisch entsprechen der technischen Entwicklung fortzuschreiben. Fehlende oder mangelhafte Massnahmen zur Gewährleistung der Datensicherheit führen grundsätzlich zu einer widerrechtlichen Datenbearbeitung, gegen welche betroffenen Personen die Rechtsansprüche gemäss Art. 25 DSG zustehen (vgl. hierzu nachfolgend E. 12.7.4). Anzumerken ist jedoch an dieser Stelle, dass eine (detaillierte) Bekanntgabe der getroffenen organisatorischen und technischen Massnahmen an betroffene Personen grundsätzlich nicht in Betracht kommen kann, ohne dass die Sicherheitsziele gefährdet würden.

An der Verpflichtung, die Datensicherheit zu gewährleisten, ändert eine allfällige Übertragung der Datenbearbeitung oder Teilen davon an Dritte nichts. Nach Art. 10a Abs. 1 DSG darf die Bearbeitung von Personendaten durch Vereinbarung oder Gesetz Dritten übertragen werden; darüber, wer unter den Begriff des Dritten fällt und wann entsprechend von einer Datenbearbeitung durch Dritte – im Gegensatz zur bloss internen Zuständigkeitsverteilung – auszugehen ist, darüber bestehen in der Literatur unterschiedliche Meinungen (vgl. BAERISWYL, a.a.O., Art. 10a Rz. 11 mit dem nachvollziehbaren Argument, es sei jeweils anhand der Organisationsstruktur des Datenbearbeiters zu prüfen, ob eine Datenbearbeitung durch einen [weisungsungebundenen] Dritten vorliegt; in diesem Sinne auch EPINEY/FASNACHT, in: Belser/Epiney/Waldmann [Hrsg.], Datenschutzrecht, 2011, § 10 Rz. 38; anders BÜHLER/RAMPINI, in: Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, Art. 10a DSG Rz. 6 f.). Voraussetzung für die (teilweise) Übertragung der Datenbearbeitung an Dritte ist, dass die Daten nur so bearbeitet werden, wie der Auftraggeber den Dritten hierzu ermächtigt. Zudem dürfen keine gesetzlichen oder vertraglichen Geheimhaltungsinteressen die Übertragung verbieten und eine Bearbeitung der Personendaten zu eigenen Zwecken durch den Dritten muss ausgeschlossen sein; würden die Personendaten (auch) für Zwecke des Dritten bearbeitet, ginge die Datenbearbeitung über eine "Datenbearbeitung durch Dritte" i.S.v. Art. 10a DSG hinaus und bedürfte eines eigenen Rechtfertigungsgrundes bzw. der Einhaltung der Voraussetzungen von Art. 19 DSG (DAVID ROSENTHAL, in: Rosenthal/Jöhri, Handkommentar zum

Datenschutzgesetz, 2008, Art. 10a Rz. 14 und 26; YVONNE JÖHRI, in: Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, 2008, Art. 16 Rz. 11). Schliesslich muss sich der Auftraggeber insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG; vgl. zu den Voraussetzungen der Auslagerung BAERISWYL, a.a.O., Art. 10a Rz. 18–40; BÜHLER/RAMPINI, a.a.O., Art. 10a DSG Rz. 11–15a). Im Gesetz zwar nicht ausdrücklich erwähnt, aber mitumfasst, ist die Pflicht des Auftraggebers, sich um die Einhaltung des Datenschutzes und damit auch der anderen allgemeinen Datenschutzgrundsätze aktiv zu bemühen (ROSENTHAL, a.a.O., Art. 10a Abs. 1 Bst. a Rz. 48 f.; EPINEY/FASNACHT, a.a.O., § 10 Rz. 49). Die Umsetzung der eigenen Verpflichtungen hinsichtlich Datensicherheit ist dem Dritten zu überbinden. Nicht von vornherein gesetzlich ausgeschlossen ist die Auslagerung der Datenbearbeitung ins Ausland. Eine solche Auslagerung hätte jedoch Auswirkungen auf die Risikoanalyse, in welche auch die ausländische Rechtssituation mit einzubeziehen ist. Untersteht der Dritte dem DSG nicht, vergewissert sich das verantwortliche Organ, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten, andernfalls stellt es diesen auf vertraglichem Wege sicher (Art. 22 Abs. 3 VDSG; vgl. BÜHLER/RAMPINI, a.a.O., Art. 10a DSG Rz. 15). Der (ausländische) Dritte muss so ins Recht gefasst werden können, dass der Auftraggeber seine Verantwortung nach dem DSG vollumfänglich wahrnehmen kann. Der Auftraggeber bleibt weiterhin verantwortlich (Art. 16 Abs. 1 DSG; Art. 22 Abs. 2 VDSG). Eine Konstellation, in der eine Anbieterin Randdaten in einem Land speichert, in welchem etwa der Staat ungehindert darauf zugreifen kann, wäre somit mit dem geltenden Recht grundsätzlich nicht vereinbar bzw. würde zur Widerrechtlichkeit der Datenbearbeitung führen (vgl. auch Art. 6 Bst. b FMG, wonach, wer einen Fernmeldedienst erbringt, das anwendbare Recht einzuhalten hat, worunter auch die anwendbaren Bestimmungen von BÜPF und DSG gehören; in diesem Sinn auch BGE 141 IV 108 E. 6.1, wonach jene Anbieterinnen, die in der Schweiz ihre Dienste anbieten, den massgebenden Bestimmungen insbesondere des BÜPF unterworfen sind).

Abschliessend ist darauf hinzuweisen, dass der Grundsatz der Datensicherheit gesetzlich in Art. 7 Abs. 1 DSG verankert ist und die Anbieterinnen auch gestützt auf diese Bestimmung unmittelbar verpflichtet sind, die angemessenen technischen und organisatorischen Massnahmen zu treffen, um Personendaten gegen unbefugtes Bearbeiten zu schützen; Zweck und systematische Stellung der Bestimmung von Art. 7 Abs. 1 DSG verbieten eine Beschränkung auf einen bestimmten Adressatenkreis (STAMM-PFISTER, a.a.O., Art. 7 DSG Rz. 2).

Zusammenfassend kann somit festgehalten werden, dass die datenschutzrechtlichen Bestimmungen zur Datensicherheit auch für die Anbieterinnen gelten, soweit diese gestützt auf das BÜPF Randdaten der Telekommunikation und damit Personendaten speichern und aufbewahren. Diese Bestimmungen sind zudem hinreichend bestimmt umschrieben, wobei angesichts des Regelungsgegenstandes nicht zu beanstanden ist, dass sich der Gesetz- wie auch der Verordnungsgeber im Wesentlichen auf den Erlass finaler Bestimmungen bzw. das Festlegen von Zielen beschränkt haben, anstatt detailliert die zu treffenden Massnahmen vorzuschreiben (vgl. STAMM-PFISTER, a.a.O., Art. 7 DSG Rz. 24). Die gesetzliche Ordnung ist insofern und entgegen der Ansicht der Beschwerdeführer auch vor dem Hintergrund des Eingriffs in ihre Grundrechte nicht zu beanstanden, zumal nicht geltend gemacht wird, es sei mit der heutigen Technik und gemessen am Gefährdungspotential, das aus der Speicherung und Aufbewahrung der Randdaten der Telekommunikation resultiert, eine sichere Datenbearbeitung nicht möglich.

12.7.4 Die Rechtsprechung verlangt – wie vorstehend ausgeführt – nach weiteren Garantien zum Schutz vor Missbrauch bei der Bearbeitung von Personendaten durch die privaten Anbieterinnen (vgl. auch JAGGI, a.a.O., S. 289; zudem Art. 7–11 der Datenschutzkonvention). Demnach müssen betroffenen Personen verfahrensrechtliche Garantien wie insbesondere ein Recht auf Auskunft und Einsicht in ihre Daten zukommen und die Löschung bzw. Vernichtung der gespeicherten Daten ist verbindlich zu regeln (vgl. vorstehend E. 12.7.2; zudem in diesem Sinne BGE 140 I 381 E. 4.5). In dieser Hinsicht bringt die Gesetzgebung zur Überwachung des Post- und Fernmeldeverkehrs keine Klärung. Teilweise ergibt sich eine solche aus dem Fernmelderecht. Nach Art. 80 der Verordnung vom 9. März 2007 über Fernmeldedienste (FDV, SR 784.101.1) dürfen die Anbieterinnen Personendaten bearbeiten, soweit und *solange* dies für den Verbindungsaufbau, für die Erfüllung ihrer Pflichten nach dem BÜPF und für den Erhalt des für die entsprechenden Leistungen geschuldeten Entgelts notwendig ist. Mit Blick darauf, dass das BÜPF in Art. 15 Abs. 3 eine Aufbewahrungsdauer von einem halben Jahr vorschreibt, dürfen die Anbieterinnen nach Ablauf dieses Zeitraumes die gespeicherten Daten nicht mehr bearbeiten und damit auch nicht weiter aufbewahren; nach Art. 3 Bst. e DSG umfasst das Bearbeiten jeden Umgang mit Personendaten und damit auch das blosse Aufbewahren.

Im Weiteren ist auf die allgemeinen Datenschutzbestimmungen des DSG hinzuweisen. Art. 4 DSG regelt die bei jeder Bearbeitung von Personendaten und entsprechend auch von den Anbieterinnen zu beachtenden allgemeinen Grundsätze (BGE 138 II 346 E. 7.1; MAURER-LAMBROU/KUNZ, a.a.O., Art. 2 DSG Rz. 14; vgl. auch Art. 89 FDV, wonach das DSG gilt, soweit die FDV keine besondere Regelung enthält). Dazu gehört, dass Personendaten nur rechtmässig bearbeitet werden dürfen (Abs. 1), dass ihre Bearbeitung nach Treu und Glauben zu erfolgen hat und verhältnismässig sein muss (Abs. 2), dass Daten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Abs. 3), und dass die Beschaffung der Daten und insbesondere der Zweck ihrer Bearbeitung für die betroffenen Personen erkennbar sein muss (Abs. 4; vgl. BGE 138 II 346 E. 9.1 f.).

Die Bearbeitung von Randdaten der Telekommunikation betreffend hat der Gesetzgeber über die Verhältnismässigkeit der Dauer der Aufbewahrung bereits generell-abstrakt entschieden, indem er einen Ausgleich zwischen den grundrechtlich geschützten Interessen Betroffener und dem öffentlichen Interesse an einer wirksamen Strafverfolgung gesucht und die Aufbewahrungsdauer auf sechs Monate beschränkt hat (vgl. Botschaft BÜPF, BBl 1998 IV 4241, 4268; ferner auch die Materialien im Zusammenhang mit der Totalrevision des BÜPF: Botschaft nBÜPF, BBl 2013 2683, 2741; Votum Nationalrätin Ursula Schneider Schüttel, AB 2015 N 1154; Votum Nationalrat Jean Christophe Schwaab für die Kommission, AB 2016 N 135). Eine Speicherung bzw. Aufbewahrung von Randdaten über die gesetzlich vorgesehene Dauer von sechs Monaten hinaus ist somit grundsätzlich unverhältnismässig und aus diesem Grund sowie mit Blick auf Art. 80 FDV zudem unrechtmässig, sofern sie sich nicht aus einem anderen Grund rechtfertigen lässt. Die Randdaten der Telekommunikation dürfen somit gestützt auf Art. 15 Abs. 3 BÜPF nur während sechs Monaten aufbewahrt werden und sind nach Ablauf dieser Aufbewahrungsfrist zu löschen (Art. 4 Abs. 1 DSG e contrario). Andernfalls ist – vorbehältlich eines Rechtfertigungsgrundes für eine längere Aufbewahrung etwa i.S.v. Art. 80 FDV – grundsätzlich von einer widerrechtlichen Bearbeitung von Personendaten auszugehen.

Zur Durchsetzung dieser Pflichten und (damit) zur Verwirklichung der durch die Verfassung und die EMRK garantierten Privatsphäre sowie des Rechts auf informationelle Selbstbestimmung sind verfahrensrechtliche Garantien nötig. Entsprechend kann nach Art. 8 Abs. 1 DSG jede Person Auskunft

über die sie betreffenden, in einer Datensammlung eines Dritten bearbeiteten Daten verlangen (vgl. BGE 138 I 6 E. 7.5.2; SCHWEIZER, a.a.O., Art. 13 Rz. 85; zur Abgrenzung von datenschutzrechtlichem Auskunftsrecht und verfahrensrechtlicher Akteneinsicht vgl. etwa BGE 126 I 7 E. 2). Der Inhaber der Datensammlung muss der betroffenen Personen alle über sie in der Datensammlung vorhandenen Daten mitteilen (Art. 8 Abs. 2 Bst. a DSG). Lässt der Inhaber der Datensammlung Personendaten durch einen Dritten bearbeiten, so bleibt er grundsätzlich selbst auskunftspflichtig (Art. 8 Abs. 4 DSG). Das Auskunftsrecht kann unter Umständen eingeschränkt werden (Art. 9 DSG; vgl. zum Ganzen BGE 138 III 425 E. 5 f. und BGE 125 II 473 E. 4). Die durch die Auskunft verschaffte Kenntnis der betroffenen Person darüber, dass und welche Daten über sie bearbeitet werden, ist Voraussetzung für die Wahrnehmung ihrer weiteren Rechte und Ansprüche, insbesondere im Fall einer widerrechtlichen Bearbeitung von Personendaten (vgl. BGE 140 V 464 E. 4.2). Gegebenenfalls stehen der betroffenen Person namentlich die Ansprüche nach Art. 25 DSG zu. Sie kann demnach verlangen, dass die widerrechtliche Bearbeitung ihrer Personendaten unterlassen wird, deren Folgen beseitigt werden oder die Widerrechtlichkeit des Bearbeitens festgestellt wird (Art. 25 Abs. 1 DSG). Ferner kann sie nach Art. 25 Abs. 3 Bst. a DSG insbesondere verlangen, dass ihre Personendaten vernichtet bzw. gelöscht werden. Das Auskunftsrecht unterstützt dergestalt die in der BV niedergelegten und auch vorliegend betroffenen Grundrechte von Art. 13 BV und kann insofern als normverwirklichte Drittwirkung der Grundrechte bezeichnet werden (GRAMIGNA/MAURER-LAMBROU, in: Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, Art. 8 DSG Rz. 2). Vor diesem Hintergrund vermag das (eingeschränkte) Auskunftsrecht gemäss Art. 45 FMG i.V.m. Art. 80 f FDV jenem gemässe Art. 8 DSG nicht grundsätzlich entgegenstehen. Das Auskunftsrecht unterstützt dergestalt die in der BV niedergelegten und auch vorliegenden interessierenden Grundrechte von Art. 13 BV und kann insofern als normverwirklichende Drittwirkung der Grundrechte bezeichnet werden.

Begehren um Auskunft sowie Ansprüche nach Art. 25 DSG sind an jenes Bundesorgan zu richten, das die Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt (Art. 16 Abs. 1 DSG). Vorliegend sind die Anbieterinnen von Gesetzes wegen mit der Erfüllung der in Frage stehenden öffentlichen Aufgabe betraut und somit für den Datenschutz verantwortlich. Entsprechende Begehren sind daher (zunächst) an die Anbieterinnen zu richten (zum Begriff des Inhabers der Datensammlung gemäss

Art. 3 Bst. i DSG siehe BLACHTA, a.a.O., Art. 3 DSG Rz. 87 f.). Dies erscheint angesichts dessen, dass der Gesetzgeber ausdrücklich vorschreibt, dass die Anbieterinnen und nicht der Staat selbst die Randdaten zu speichern und aufzubewahren hat, die Anbieterinnen mithin die Verfügungsmacht über die Randdaten besitzen, auch sachgerecht.

An dieser Zuständigkeitsordnung ändert nichts, dass die Anbieterinnen keine Befugnis zum Erlass von Verfügungen besitzen. Kommt die betreffende Anbieterin dem Begehren eines Betroffenen nicht nach bzw. kann keine Einigung gefunden werden, steht es der betreffenden Person frei, an die Vorinstanz als die im Anwendungsbereich von Art. 15 Abs. 3 BÜPF zum Erlass von Verfügungen zuständige Behörde zu gelangen, welche in Anwendung des VwVG ein förmliches Verfahren auf Erlass einer Verfügung durchführt (vgl. Art. 25 Abs. 4 DSG; zudem die vergleichbare Systematik in Art. 22 Abs. 2 Bst. a des Stromversorgungsgesetzes [StromVG, SR 734.7] für den Fall, dass zwischen den [privaten] Beteiligten keine Einigung zu Stande kommt).

12.7.5 Zusammenfassend ist festzuhalten, dass das Fernmelderecht und insbesondere das Datenschutzrecht hinreichende Garantien zum Schutz vor Missbrauch bei der Bearbeitung der Randdaten der Telekommunikation der Beschwerdeführer vorsehen; die Grundsätze des Datenschutzrechts gemäss Art. 4 DSG stellen, verbunden mit den verfahrensrechtlichen Garantien gemäss Art. 8 und Art. 25 DSG, eine echte Begrenzung dar (vgl. BGE 136 I 87 E. 8.4). Zusätzlicher Schutz besteht durch die Aufsicht des EDÖB auch über die Anbieterinnen (vgl. BGE 138 I 6 E. 5.4); die Aufsicht gemäss Art. 27 DSG ist eine sachbereichsspezifische und steht der allgemeinen Aufsicht durch die Vorinstanz nicht entgegen. Anzumerken ist, dass die Randdaten der Telekommunikation insbesondere zum Zweck der Strafverfolgung gespeichert und aufbewahrt werden und vor diesem Hintergrund nicht gesagt werden kann, die Daten würden zu einem anderen Zweck bearbeitet, als was im BÜPF vorgesehen ist (vgl. Urteil des BVGer A-6320/2014 vom 23. August 2016 E. 11.3.3.2 und E. 13). Dies ist zudem mit Blick auf den Zweckartikel des BÜPF für die Beschwerdeführer in hinreichendem Mass erkennbar, weshalb auch nicht gesagt werden kann, die Speicherung und Aufbewahrung von Randdaten stehe zu weiteren Grundsätzen des Datenschutzes, etwa der Zweckbindung, in einem unlösbaren Widerspruch.

12.8 Vor dem Hintergrund des vorstehend Ausgeführten sind schliesslich die berührten Interessen, die grund- und völkerrechtlich geschützten Ansprüche der Beschwerdeführer und insbesondere das Interesse an einer wirksamen Strafverfolgung gegeneinander abzuwägen. Dabei ist in Betracht zu ziehen, dass insbesondere das Datenschutzrecht verschiedene Garantien zum Schutz vor einer missbräuchlichen Verwendung der Personendaten vorsieht. Die Aufbewahrungsdauer ist beschränkt und es gelten für die Anbieterinnen verbindliche Vorschriften bezüglich Datensicherheit, deren Einhaltung auch der Aufsicht durch den EDÖB unterstellt ist. Die geschützten Rechtspositionen der Beschwerdeführer sind zudem verfahrensrechtlich abgesichert durch ein Auskunftsrecht sowie – im Fall einer widerrechtlichen Datenbearbeitung – durch die Ansprüche gemäss Art. 25 DSG. Die Bearbeitung der Randdaten ist (somit) sachlich und zeitlich begrenzt und die Missbrauchsgefahr minimiert (vgl. auch BGE 138 I 6 E. 7.7). Auf der anderen Seite steht insbesondere das gewichtige öffentliche und private Interesse an einer wirksamen Strafverfolgung; Geschädigte, Dritte und u.U. die Betroffenen selbst haben ein berechtigtes Interesse an der Aufklärung von strafrechtlich relevanten Sachverhalten (BGE 138 I 256 E. 5.5). Den geschützten Rechtspositionen der Beschwerdeführer kommt vor diesem Hintergrund und mit Blick auf ein offenkundig teilweise gewandeltes gesellschaftliches Bewusstsein im Umgang mit moderner Informationstechnologie (vgl. BGE 138 II 346 E. 10.6.6), auch wenn durch die Verfassung ausgewiesen, nicht dasselbe Gewicht zu wie dem Interesse an einer wirksamen Strafverfolgung von Verbrechen und Vergehen, d.h. bei Tatvorwürfen wie etwa Tötung, sexuelle Handlungen mit Kindern oder Abhängigen, sexuelle Nötigung, Vergewaltigung, Pornographie, Körperverletzung, Verleumdung (Antragsdelikt), Drohung, Freiheitsberaubung, Geiselnahme, Hausfriedensbruch (Antragsdelikt), Diebstahl, Raub, Erpressung, Brandstiftung, Urkundenfälschung oder in der Regel bei Verstössen gegen das Betäubungsmittelgesetz (BetmG, SR 812.121). Der vom Gesetzgeber zwischen den betroffenen Rechtsgütern getroffene abstrakte Ausgleich ist insofern nicht zu beanstanden.

An diesem Ergebnis vermögen insbesondere mit Blick auf die gesetzlich vorgesehenen Mechanismen zum Schutz vor Missbrauch weder die Anlasslosigkeit der Speicherung noch der Umfang der gespeicherten Daten etwas zu ändern (vgl. BGE 140 I 353 E. 4.7.2; BGE 138 II 346 E. 10, insbes. E. 10.7). Dasselbe gilt für den Umstand, dass im Rahmen einer rückwirkenden Überwachung u.U. auch Personendaten Dritter bekannt gegeben werden; eine solche allfällige Beeinträchtigung der Privatsphäre Dritter ist ein jeder Überwachung der Telekommunikation innewohnendes Risiko

(vgl. das Urteil des BGer vom 21. März 1989 in Sachen Generaldirektion PTT ggn. Untersuchungsrichter und Anklagekammer des Kantons Genf, publiziert in Pra 1989 Nr. 211, E. 5b). Zudem ist keine unverhältnismässige abschreckende Wirkung i.S. eines Chilling Effects auszumachen. Die mit der Speicherung und Aufbewahrung von Randdaten der Telekommunikation verbundene Einschränkung der Grundrechte der Beschwerdeführer ist somit zumutbar und verhältnismässig bzw. in einer demokratischen Gesellschaft notwendig.

12.9 Die Einschränkung der grund- und völkerrechtlich geschützten Vertraulichkeit der Kommunikation sowie des Rechts der Beschwerdeführer auf informationelle Selbstbestimmung stützt sich nach dem Gesagten auf eine hinreichend bestimmte gesetzliche Grundlage, ist durch ein öffentliches Interesse gerechtfertigt und verhältnismässig. Zudem ist insbesondere vor dem Hintergrund der im DSG vorgesehenen Garantien zum Schutz vor Missbrauch nicht ersichtlich und wird auch nicht vorgebracht, dass mit der Speicherung und Aufbewahrung der Randdaten in den Kernbereich von Art. 13 Abs. 1 und 2 BV eingegriffen würde. Die Grundrechtseinschränkung erweist sich somit als zulässig.

Unschuldsvermutung / Medienfreiheit

13.
Die Beschwerdeführer berufen sich ferner auf die Unschuldsvermutung, wie sie in Art. 32 Abs. 1 BV umschrieben ist. Sie sehen diese dadurch verletzt, dass anlasslos und systematisch die Randdaten der Telekommunikation gespeichert und aufbewahrt werden. In diesem Zusammenhang rügen sie auch eine Verletzung des strafprozessualen nemo-tenetur-Prinzips und zwei der Beschwerdeführer, die als Journalisten tätig sind, machen geltend, die strafprozessualen Bestimmungen würden den Quellenschutz nicht in hinreichendem Masse gewährleisten, da die Strafverfolgungsbehörden unter Umständen doch Kenntnis von einer Quelle erhielten.

Art. 32 BV schützt unter dem Titel Strafverfahren die Grundrechte des Angeschuldigten und umfasst nebst der Unschuldsvermutung (Abs. 1) auch Informationsrechte (Abs. 2) und eine Rechtsmittelgarantie (Abs. 3). Die grundrechtliche Garantie der Unschuldsvermutung verlangt insbesondere, dass die Schuld eines Angeklagten in einem Verfahren vor dem zuständigen Gericht nachgewiesen wird. Ihre zentrale Bedeutung hat die Unschuldsvermutung im Beweisrecht; der Grundsatz von Art. 32 Abs. 1 BV

enthält eine Beweislast und eine Beweiswürdigungsregel (vgl. hierzu MÜLLER/SCHEFER, a.a.O., S. 981–984). Darüber hinaus schützt es den Angeschuldigten vor Zwangsmassnahmen, die eine aktive Mitwirkung an seiner eigenen Überführung voraussetzen würden (nemo-tenetur-Prinzip; hierzu HANS VEST, in: St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 32 Rz. 8 mit Hinweisen auch auf die Rechtsprechung des EGMR).

Die Speicherung und Aufbewahrung von Randdaten der Telekommunikation steht nicht in einem unmittelbaren Zusammenhang mit einem Strafverfahren. Daran ändert auch nichts, dass Speicherung und Aufbewahrung im Hinblick auf eine allfällige Strafuntersuchung erfolgen und insofern auch eine Beweissicherungsmassnahme darstellen. Die blosse Speicherung und Aufbewahrung führt für sich zu keiner Anschuldigung im strafprozessualen Sinn (vgl. BGE 138 I 256 E. 4). Vielmehr setzt der Zugriff der Strafverfolgungsbehörden auf die Randdaten voraus, dass bereits ein anderweitig begründeter Verdacht besteht (vgl. Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 Bst. a StPO) und die Untersuchungsmassnahme bedarf der Zustimmung durch das Zwangsmassnahmengericht (Art. 273 Abs. 2 StPO). Ein Schuldvorwurf im strafrechtlichen Sinn ist daher mit der blossen Speicherung und Aufbewahrung der Randdaten nicht verknüpft. Und auch ein unzulässiger Zwang im Sinne der Rechtsprechung zum nemo-tenetur-Prinzip, sich selbst zu belasten, ist nicht ersichtlich. Es ist aus diesen Gründen und auch mit Blick auf die Trennung der verwaltungsrechtlichen von den strafprozessualen Aspekten der Überwachung des Post- und Fernmeldeverkehrs nicht ersichtlich, dass die Beschwerdeführer in ihren durch Art. 32 BV geschützten Ansprüchen beeinträchtigt wären (vgl. auch vorstehend E. 8.2). Dasselbe gilt für die Medienfreiheit gemäss Art. 17 BV, welche die Beschwerdeführer im Zusammenhang mit dem ihrer Ansicht nach unzureichenden journalistischen Quellenschutz im Strafverfahren anrufen. Diese Vorbringen sind nicht im vorliegenden Verfahren, sondern in einem allfälligen Strafprozess zu erheben (vgl. vorstehen E. 8.4 sowie im Ergebnis etwa das Urteil des BGer 1B_424/2013 vom 22. Juli 2014 E. 6). Die Beschwerden erweisen sich auch vor diesem Hintergrund als unbegründet.

14.

Nicht weiter einzugehen ist auf die weiteren ausländischen (verfassungsrechtlichen) Urteile und Dokumente, auf welche die Beschwerdeführer mit Eingabe vom 24. April 2015 hinweisen. Es ist nicht ersichtlich und wird auch nicht konkret geltend gemacht, dass diese über das bereits Ausgeführte hinaus für die vorliegende Streitsache von Bedeutung wären. Das-

selbe gilt für die Eingabe vom 6. November 2015 an das deutsche Bundesverfassungsgericht in Karlsruhe, welche die Beschwerdeführer dem Bundesverwaltungsgericht mit Schreiben vom 23. Februar 2016 beigebracht haben.

Aus denselben Gründen sind schliesslich die Anträge der Beschwerdeführer, es seien die sie betreffenden Randdaten beizuziehen, in vorwegnehmender Beweiswürdigung abzuweisen (vgl. Urteil des BVGer A-1251/2012 vom 15. Januar 2014 E. 8.2; zur Frage, welche Randdaten gestützt auf Art. 15 Abs. 3 BÜPF gespeichert und aufbewahrt werden müssen vgl. vorstehend E. 9.3). Somit kann offen blieben, inwieweit die Anbieterinnen im vorliegenden Verfahren hätten dazu verpflichtet werden können, dem Bundesverwaltungsgericht den Fernmeldeverkehr der Beschwerdeführer betreffende Randdaten herauszugeben.

15.
Insgesamt ist somit festzuhalten, dass die Anbieterinnen in Erfüllung einer öffentlichen Aufgabe des Bundes zwar in grund- und völkerrechtlich geschützte Positionen der Beschwerdeführer – das Recht auf Vertraulichkeit ihrer Kommunikation und in ihr Recht auf informationelle Selbstbestimmung – eingreifen, die Einschränkung jedoch mit Art. 15 Abs. 3 BÜPF in hinreichend bestimmter Weise im Gesetz selbst vorgesehen, durch das öffentliche Interesse an einer wirksamen Strafverfolgung gerechtfertigt und mit Blick insbesondere auf die im Datenschutzrecht vorgesehenen Mechanismen zum Schutz vor Missbrauch von Personendaten auch verhältnismässig ist. Die Beschwerden sind daher als unbegründet abzuweisen.

Kosten

16.
Das Bundesverwaltungsgericht auferlegt die Verfahrenskosten in der Regel der unterliegenden Partei (Art. 63 Abs. 1 VwVG). Die Gerichtsgebühr bemisst sich insbesondere nach Umfang und Schwierigkeit der Streitsache (Art. 2 Abs. 1 des Reglements vom 21. Februar 2008 über die Kosten und Entschädigungen vor dem Bundesverwaltungsgericht [VGKE, SR 173.320.2]).

Das Bundesverwaltungsgericht setzt vorliegend die Kosten für die Durchführung der vereinigten Beschwerdeverfahren einschliesslich der Kosten für die Zwischenverfügung vom 6. Mai 2015 in Anwendung von Art. 1 ff.

VGKE auf insgesamt Fr. 6'000.– fest, wovon den unterliegenden Beschwerdeführern je Fr. 1‘000.– zur Bezahlung aufzuerlegen sind. Die jeweils in derselben Höhe geleisteten Kostenvorschüsse sind zur Bezahlung der Verfahrenskosten zu verwenden.

Den Beschwerdeführern steht angesichts ihres Unterliegens keine Parteientschädigung zu (Art. 64 Abs. 1 VwVG und Art. 7 Abs. 1 VGKE e contrario).

Demnach erkennt das Bundesverwaltungsgericht:

1.
Die Beschwerden werden abgewiesen.

2.
Die Verfahrenskosten von Fr. 6‘000.– werden den Beschwerdeführern in der Höhe von je Fr. 1‘000.– zur Bezahlung auferlegt. Die jeweils in der Höhe von Fr. 1‘000.– geleisteten Kostenvorschüsse werden jeweils zur Bezahlung der Verfahrenskosten verwendet.

3.
Es werden keine Parteientschädigungen zugesprochen.

4.
Dieses Urteil geht an:

– die Beschwerdeführer (Gerichtsurkunde)
– die Vorinstanz (Gerichtsurkunde)
– das Generalsekretariat EJPD (Gerichtsurkunde)

Für die Rechtsmittelbelehrung wird auf die nächste Seite verwiesen.

Die vorsitzende Richterin:	Der Gerichtsschreiber:
Christine Ackermann	Benjamin Kohle

Rechtsmittelbelehrung:

Gegen diesen Entscheid kann innert 30 Tagen nach Eröffnung beim Bundesgericht, 1000 Lausanne 14, Beschwerde in öffentlich-rechtlichen Angelegenheiten geführt werden (Art. 82 ff., 90 ff. und 100 BGG). Die Rechtsschrift ist in einer Amtssprache abzufassen und hat die Begehren, deren Begründung mit Angabe der Beweismittel und die Unterschrift zu enthalten. Der angefochtene Entscheid und die Beweismittel sind, soweit sie der Beschwerdeführer in Händen hat, beizulegen (Art. 42 BGG).

Versand: