

EINGEGANGEN

15. Nov. 2016

FRIST:.....



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.

2.

3.

4.

5.

6. |

alle vertreten durch lic. iur. Viktor Györfy, Rechtsanwalt,
Peyrot, Schlegel und Györfy 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.**

Balthasar Glättli, Hernani Marques Madeira, Erik Schönenberger, Etrit Hasler, Dominique Strelbel und Norbert Bollow (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 ermitteln 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 Dominique Strelbel sowie Etrit Hasler, 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 angebehrten 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 ermitteln, 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 (formell-gesetzlichen) 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 milderer 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 dienen 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, inwieweit nach Ermittlungsbeginn rückwirkende Überwachungen in der Regel angeordnet würden.

G.

Mit Zwischenverfügung vom 6. Mai 2015 weist der Instruktionsrichter ein Gesuch der Beschwerdeführer vom 2. Februar 2015, es seien ihre Beschwerdeverfahren zu sistieren, ab, da keine hinreichenden Gründe für eine Trennung der Beschwerdeverfahren und die angebehrte 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, Staatschutz oder Datenschutz?, 2014, S. 186 ff.; zudem und auch zur Gegen Ausnahme 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 streitbetreffenen 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 Rechtshilfsersuchen 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 streitbetreffene 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 Rechtsweg 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 Rechtsweg 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 insofern 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 Fernmeldeleistungen 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 procédure 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 auskunftsberechtigten 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 Fernmeldeverkehr, sondern stehen lediglich im Zusammenhang mit Fernmeldeanschlüssen, 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 Rechtsfehler 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 (BVG E. 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-