Eidgenössisches Justiz- und Polizeidepartement EJPD

Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Recht und Controlling

A CH-3003 Bern
ISC-EJPD

Einschreiben

Vorname Name
Strasse Nr.
Postleitzahl Ort

Unser Zeichen: kor
Sachbearbeiter/in: René Koch
Bern, 30. Juni 2014

Verfügung

des

Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF)

in der Sache

Vorname Name, geb. TT.MM.JJJJ, Strasse Nummer, Postleitzahl Ort (Gesuchsteller)
vertreten durch Rechtsanwalt Vorname Name, Strasse Nummer, Postleitzahl Ort

betreffend Gesuch vom 20. Februar 2014 zur Vorratsspeicherung von Randdaten der Fernmeldekommunikation

Informatik Service Center ISC-EJPD
René Koch
Fellerstrasse 15, 3003 Bern
www.isc-ejpd.admin.ch

I. SACHVERHALT

Am 20. Februar 2014 hat der Gesuchsteller beim Dienst ÜPF folgende Anträge gestellt:

«1. Die Fernmeldedienstanbieterin X sei anzuweisen, die gemäss Art. 15 Abs. 3 ÜPF [richtig: BÜPF] 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 Fernmeldedienstanbieterin X sei anzuweisen bzw. zu verpflichten, keine gemäss Art. 15 Abs. 3 ÜPF [richtig: BÜPF] gespeicherten Verkehrs- und Rechnungsdaten des Gesuchstellers an den Dienst ÜPF oder an andere Behörden oder an Gerichte herauszugeben;

unter Kosten- und Entschädigungsfolgen zu Lasten des Staates.»

Als Begründung führt der Gesuchsteller Grundrechtseingriffe auf, welche seines Erachtens durch die Datenspeicherung verursacht werden und nicht gerechtfertigt sind.

Die Fernmeldedienstanbieterin X ist Fernmeldedienstanbieterin. Sie speichert Verkehrs- und Rechnungsdaten (im Folgenden: Randdaten) des Fernmeldeverkehrs ihrer Kunden, die Mobil- und Festnetzanschlüsse für Telefon- und Internetverbindungen oder Internetdienste benützen. Diese Daten speichert sie, um sie einer zuständigen Behörde übermitteln zu können, wenn diese eine entsprechende Überwachungsanordnung erlässt (sogenannte Vorratsdatenspeicherung). Die Daten erlauben der jeweiligen Behörde eine rückwirkende Überwachung gewisser Aspekte der Kommunikation und des sonstigen Verhaltens der betreffenden Personen. Der Gesuchsteller ist Kunde der Fernmeldedienstanbieterin X.

II. ERWÄGUNGEN

A. FORMELLES

1. Der Gesuchsteller verlangt, dass in Konkretisierung von Artikel 15 BÜPF gegenüber der Fernmeldedienstanbieterin X ein Verbot ausgesprochen werde.

2. Zuständige Behörde für den Erlass einer Verfügung nach Artikel 15 Absatz 3 BÜPF ist der Dienst ÜPF. Das BÜPF sieht zwar den Erlass von Verfügungen wie der vorliegenden nicht ausdrücklich vor – anders als bei den Verfügungen über die Umsetzung konkreter Überwachungsanordnungen (Art. 13 Abs. 1 Bst. b BÜPF). Es ergibt sich aus dem Gesetz aber, dass der Dienst ÜPF die für die Fernmeldeüberwachung zuständige Behörde ist (Art. 2 Abs. 1 BÜPF). Das Bundesamt für Kommunikation (BAKOM) hat zwar die allgemeine Aufsicht über die Fernmeldedienstanbieterinnen (Art. 58 des Fernmeldegesetzes vom 30. April 1997, FMG, SR 784.10). Nach Absatz 1 dieser Bestimmung ist die Aufsicht des BAKOM aber auf das Fernmelderecht beschränkt, konkreter auf der Stufe des Bundesgesetzes: auf das Fernmeldegesetz. Das BAKOM ist daher nicht zuständig für das vorliegende Aufsichtsverfahren, in dem es um die Erfüllung einer spezifisch aus dem BÜPF fliessenden Pflicht geht.

3. Der Gesuchsteller als Dritter kann die Verfügung nur verlangen, wenn er ein schutzwürdiges Interesse im Sinne von Artikel 48 Absatz 1 Buchstabe c VwVG hat (in Verbindung mit Art. 6 VwVG; vgl. dazu BGE 98 Ib 53 E. 3; 120 Ib 351 E. 3a). Weil das verlangte Verbot staatlich veranlasste Eingriffe in Grundrechte des Gesuchstellers betrifft, ist das schutzwürdige Interesse zu bejahen.

4. Bezüglich des Begehrens 2 besteht hingegen kein hinreichendes aktuelles schutzwürdiges Interesse. Der Rechtsschutz bei konkreten Überwachungen ist gesetzlich geregelt (nachträgliche Information und Beschwerdemöglichkeit nach Art. 279 StPO). Es wäre gar nicht möglich, vorweg eine Interessenabwägung vorzunehmen, ohne die Gründe für eine konkrete Überwachung zu kennen.

5. Folglich ist auf das Begehren 1 (Speicherung einstellen/unterlassen; vorhandene Daten löschen) einzutreten. Nicht einzutreten ist hingegen auf das Begehren 2 (Herausgabe an Behörden unterlassen).

B. MATERIELLES

Fernmeldegeheimnis

6. **Eingriff in den Schutzbereich:** Das Grundrecht auf Achtung des Fernmeldegeheimnisses (Teilgehalt von Art. 13 Abs. 1 BV) folgt dem Grundgedanken, dass die Kommunikation mit fremden Mitteln wie Post, Telefon und Telegrafie gegenüber Drittpersonen geheim erfolgen können soll. Immer dann, wenn die Kommunikation durch eine Organisation erfolgt, soll sie im Vertrauen auf die Respektierung der Geheimsphäre vertraulich geführt werden können, ohne dass das Gemeinwesen Kenntnis und Einblick erhält und daraus gewonnene Erkenntnisse gegen den Betroffenen verwendet (BGE 126 I 50 E. 6.a). Dieses Grundrecht schützt die Kommunikation unabhängig vom verwendeten Kommunikationsmedium, also auch beim Einsatz verschiedenster internetbasierter Kommunikationskanäle (Jörg Paul Müller / Markus Schefer, Grundrechte in der Schweiz, 4. Auflage Bern 2008, S. 203).

7. Die Verpflichtung der privaten Anbieterinnen, Daten ihrer Kunden zu speichern, führt zwar nicht direkt dazu, dass staatliche Organe Zugriff darauf erhalten. Sie ist jedoch durch das Gesetz auf genau diesen Zweck hin zugeschnitten. Anzumerken ist jedoch, dass die Anbieterinnen von Fernmeldediensten ohnehin alle oder einen Teil der betreffenden Daten vor allem aus geschäftlichen Gründen und zum Zwecke der Rechnungsstellung aufbewahren.

8. Die heute von breiten Bevölkerungskreisen eingesetzten elektronischen Kommunikationsmittel lassen umfangreiche Mengen von Randdaten entstehen. So wird insbesondere beim Einsatz von mobilen, internetfähigen Endgeräten (heute v.a.: Smartphones und Tablets) nicht nur aufgezeichnet, wann der Benutzer bewusst jemanden angerufen oder jemandem eine Botschaft geschickt hat oder einen Anruf oder eine Botschaft erhalten hat. Vielmehr werden auch zahlreiche mehr oder weniger automatisierte Kommunikationsvorgänge registriert, die beispielsweise dazu dienen, Informationen über das Wetter oder über Sportresultate abzurufen. Zusätzlich gehört zu den Randdaten mobiler Kommunikation auch die Information, wo sich das Endgerät jeweils befand. Somit entsteht eine grosse Menge von Daten mit hoher Aussagekraft. Die aufgezeichneten Randdaten erlauben einen tiefen Einblick in das Privatleben, insbesondere in die sozialen Beziehungen der betreffenden Personen.

9. Zudem ist auch die Zweckbestimmung der Datensammlung zu berücksichtigen. Diese liegt in der Vorbereitung auf eine mögliche rückwirkende und geheime Überwachung des Kommunizierenden. Dieser Umstand ist geeignet, das Vertrauen der Menschen in die Kommunikationsinfrastruktur zu beeinträchtigen.

10. Vor diesem Hintergrund ist der Eingriff in das grundrechtlich geschützte Fernmeldegeheimnis als schwer im Sinn von Artikel 36 Absatz 1 zweiter Satz BV zu betrachten.

11. Eine Verletzung des **Kerngehalts** (Art. 36 Abs. 4 BV) des grundrechtlich geschützten Fernmeldegeheimnisses liegt nicht vor.

12. Nach Artikel 36 Absätze 1–3 BV setzt die **Rechtfertigung des Grundrechtseingriffs** voraus, dass eine genügende gesetzliche Grundlage dafür besteht, dass der Eingriff durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt ist und dass er verhältnismässig ist. Die Verhältnismässigkeit ist gewahrt, wenn der Eingriff zur Wahrung der verfolgten Interessen geeignet und erforderlich ist und diese Interessen gegenüber dem Eingriff überwiegen.

13. **Gesetzliche Grundlage:** Die Speicherung der Randdaten stützt sich auf Artikel 15 Absatz 3 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1) und die betreffenden Ausführungsbestimmungen. Die Dauer der Speicherung ist auf sechs Monate festgelegt.

14. Die Fernmeldedienstanbieterin X ist durch das zuständige BAKOM als Fernmeldedienstanbieterin eingetragen und wird vom Geltungsbereich des BÜPF erfasst, weshalb sie in der Lage sein muss, ihre Pflichten nach BÜPF und VÜPF wahrzunehmen.

15. Die gespeicherten Randdaten umfassen nach dem Gesetzeswortlaut Verkehrs- und Rechnungsdaten. Nach Artikel 16 Buchstabe d der Verordnung vom 31. Oktober 2011 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11) sind bei Telefondiensten im Einzelnen folgende Daten zu speichern, sofern es zum Aufbau einer Kommunikation gekommen ist:

a. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldedienstanbieterin bekannt sind);

b. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die IMSI-Nummer und die IMEI-Nummer);

c. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist;

d. das Datum, die Zeit und die Dauer der Verbindung.

16. Bei der Überwachung des Internets sind nach Artikel 24*b* VÜPF die Daten zu speichern, die folgende rückwirkende Überwachungsmassnahmen ermöglichen:

a. die Übermittlung der folgenden Angaben über den überwachten Zugang:

1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wurde,

2. die Art der Datenverbindung oder des Anschlusses,

3. die verwendeten Anmeldungsdaten (Log-in),

4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation,

5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (z.B. MAC-Adresse, IMEI-Nummer, IMSI-Nummer),

6. bei Zugang über ein Mobilfunknetz: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,

b. die Übermittlung der folgenden Angaben bei Versand oder Empfang von Meldungen durch einen asynchronen elektronischen Postdienst:

1. das Datum und die Uhrzeit des Versands oder des Empfangs von Mitteilungen bei der Internetzugangsanbieterin,

2. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss benutztem Protokoll,

3. die IP-Adressen der sendenden und empfangenden Fernmeldeanlagen der asynchronen elektronischen Postdienste,

4. die anderen verfügbaren Adressierungselemente.

17. Der Bundesrat kann sich zum Erlass dieser Regelung auf Artikel 15 Absatz 6 BÜPF stützen (vgl. das Gutachten des Bundesamts für Justiz vom 16. April 2010, VPB 1/2012, insb. Ziff. 2.2.4).

18. Die technischen und organisatorischen Einzelheiten sind gestützt auf Artikel 33 Absatz 1bis VÜPF in den Richtlinien des Dienstes ÜPF "technical requirements for telecommunication surveillance" (TR TS) vom 9. November 2012, Version 3.1, Kapitel 10 sowie "organisational and administrativ requirements" (OAR) vom 9. November 2012, Version 2.14 konkretisiert (die Richtlinien des Dienstes ÜPF sind abrufbar unter www.li.admin.ch).

19. Aufgrund des Fernmeldegeheimnisses darf die Fernmeldedienstanbieterin Dritten keine Einsicht in die gespeicherten Daten geben (Art. 43 FMG, Art. 321ter StGB). Die Herausgabe der Daten an Behörden ist in Straf- und Rechtshilfeverfahren sowie zur Suche Vermisster zulässig (Art. 1 Abs. 1 und Art. 3 BÜPF, Art. 273 StPO, Art. 18*a* und 18*b* des Rechtshilfegesetzes vom 20. März 1981, IRSG, SR 351.1). Für eine solche rückwirkende Überwachung ist jeweils die Anordnung der zuständigen Behörde erforderlich (im Strafverfahren: der Staatsanwaltschaft, Art. 273 Abs. 1 StPO; siehe für das Rechtshilfeverfahren Art. 55 StPO und Art. 17 und 78 f. IRSG). Die Anordnung bedarf zudem der Genehmigung durch ein Gericht (Art. 273 Abs. 2 StPO, Art. 18*a* Abs. 3 und Art. 18*b* Abs. 1 Bst. b IRSG, Art. 3 Abs. 3 und 4 BÜPF). In Straf- und Rechtshilfeverfahren darf die Überwachung nur angeordnet werden, wenn a) der dringende Verdacht besteht, ein Verbrechen oder Vergehen oder eine Übertretung nach Artikel 179^{septies} StGB sei begangen worden, b) die Schwere der Straftat die Überwachung rechtfertigt und c) die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden (Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 Bst. b und c StPO; Art. 18*a* Abs. 4 IRSG; vgl. zum etwas anders gelagerten System nach Art. 18*b* Abs. 1 Bst. a IRSG und die Gewährleistung eines adäquaten Rechtsschutzes BBl 2010 4697, 4733–4736). Zur Suche Vermisster ist die Überwachung zulässig, wenn die Polizei den Aufenthalt der betreffenden Person als unbekannt festgestellt hat und dringende Anhaltspunkte für eine schwere Gefährdung ihrer Gesundheit oder ihres Lebens bestehen (Art. 3 Abs. 1 BÜPF). Für Fälle, in denen Berufsgeheimnisse betroffen sind, sind besondere Sicherungsmassnahmen vorgesehen (Art. 271 StPO).

20. Den anwendbaren Bundesgesetzen ist somit nicht nur die Grundentscheidung des Gesetzgebers für die Vorratsdatenspeicherung zu entnehmen, sondern der Gesetzgeber bestimmt auch im Grundsatz, welche Daten zu speichern sind (Verkehrs- und Rechnungsdaten). Ebenso schreibt er vor, dass die Daten vertraulich zu behandeln und zu schützen sind und unter welchen Voraussetzungen sie an Behörden weitergegeben werden können. Dabei sieht er hohe verfahrensrechtliche Hürden vor. Somit ist die für den schweren Grundrechtseingriff nötige Grundlage auf Gesetzesstufe vorhanden (vgl. Art. 36 Abs. 1 zweiter Satz BV). Auf Verordnungs- und Richtlinienstufe wird sodann der Umfang der zu speichernden Daten weiter konkretisiert. Insgesamt ergibt sich daraus eine relativ dichte Normierung, die den Anforderungen an die Bestimmtheit der gesetzlichen Grundlage genügt.

21. Der Gesuchsteller rügt zwar, die anwendbaren Erlasse erlaubten es ihm nicht, effektiv zu ermessen, welche Daten über ihn gespeichert würden und welche Informationen damit gewonnen würden (Gesuch Ziff. II.A.3–4, II.B.6–11). Angesichts der hohen technischen Komplexität der Materie kommen jedoch der Verordnungsgeber sowie der Dienst als Autor der Richtlinien nicht umhin, sich einer präzisen, technischen Sprache zu bedienen. Dass der technische Laie sich als Normadressat nicht ohne Weiteres aufgrund der anwendbaren Regelung von allen technischen Details der Randdatenspeicherung ein genaues Bild machen kann, liegt nicht an einer mangelnden Präzision oder Transparenz der Regelung, sondern an der Komplexität der von den Fernmeldedienstanbieterinnen angebotenen und von ihren Kunden genutzten technischen Dienstleistungen. Artikel 16 Buchstabe d und Artikel 24*b* VÜPF stecken den Rahmen der zu speichernden Daten in einer auch für interessierte Laien zugänglichen Sprache ab. Die Adressaten können sich aufgrund dessen ein Bild davon machen, wie gross der Umfang der über sie gespeicherten Daten ist.

22. Folglich ist eine genügende gesetzliche Grundlage für die vorgenommene Vorratsdatenspeicherung vorhanden.

23. Mit der Vorratsdatenspeicherpflicht verfolgt der Staat das **öffentliche Interesse**, dass die Behörden Straftaten bekämpfen und Vermisste suchen können. In vielen Fällen dient die rückwirkende Überwachung, die durch die gespeicherten Daten ermöglicht wird, zudem dem **Schutz von Grundrechten Dritter**.

24. Eine rückwirkende Überwachung mittels gespeicherter Randdaten ist grundsätzlich **geeignet**, zur Bekämpfung von Straftaten und zur Suche nach Vermissten beizutragen. Informationen darüber, wer wann mit wem kommuniziert hat, wo sich die Kommunikationspartner befanden und welche Kommunikationsmittel sie einsetzten, können helfen, strafbares Verhalten im Nachhinein nachzuvollziehen oder den Aufenthaltsort vermisster Personen zu ermitteln.

25. **Erforderlichkeit**: Der Grundrechtseingriff gilt dann als erforderlich, wenn kein gleich wirksames, milderes Mittel zur Wahrung der betreffenden Interessen vorhanden ist. Im Grundsatz ist dazu festzuhalten, dass die Vorratsdatenspeicherung und die dadurch ermöglichte rückwirkende Überwachung Ermittlungsmöglichkeiten eröffnen, die ohne sie nicht bestehen würden.

26. Zudem ist auf die Regeln hinzuweisen, die für den Zugriff auf die Daten und deren Verwendung für eine rückwirkende Überwachung gelten. Die zuständigen Behörden dürfen eine Überwachung in Straf- und Rechtshilfeverfahren nur anordnen, wenn die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden (Art. 273 Abs. 1 i.V.m. Art. 269 Abs. 1 Bst. c StPO; Art. 18*a* Abs. 4 IRSG). Das dient dazu, Überwachungen auszuschliessen, für die zwar die schematischen Anforderungen nach der Gesetzgebung erfüllt wären, die aber aufgrund der Umstände des Einzelfalls nicht erforderlich sind.

27. Zur prozeduralen Absicherung dieser Regelung verlangt das Gesetz, dass die Staatsanwaltschaft (und nicht die ermittelnde Polizei) die Überwachung anordnet und die Anordnung zusätzlich dem Zwangsmassnahmengericht zur Genehmigung unterbreiten muss (Art. 273 Abs. 1 und 2 StPO, Art. 18*a* Abs. 3 IRSG). Auch bei der Suche nach Vermissten ist eine gerichtliche Genehmigung erforderlich (Art. 3 Abs. 3 und 4 BÜPF).

28. Damit sieht das schweizerische Gesetz im Unterschied zur gerichtlich für ungültig erklärten EU-Richtlinie eine Beschränkung auf das Notwendige vor (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 vom 13.04.2006; Urteil des Europäischen Gerichtshofs C-293/12 und C-594-12 vom 8. April 2014, E. 51–69.). Der Grundrechtseingriff ist aufgrund der hierzulande geltenden Gesetzgebung mit anderen Worten erforderlich, um die oben genannten öffentlichen und privaten Interessen zu wahren.

29. Zur **Interessenabwägung** (Verhältnismässigkeit im engeren Sinn) ist zunächst an die Schwere des Eingriffs in das Grundrecht der betroffenen Personen zu erinnern (s.o. Ziff. 6–10). Dem tiefen Einblick in das Privatleben, den die heute möglichen, umfangreichen Datensammlungen ermöglichen, steht das ebenfalls bereits thematisierte gewichtige Interesse an Strafverfolgung und Notsuche gegenüber. Dieses wiederum wird dadurch gesteigert, dass die verschiedenen modernen Kommunikationsmöglichkeiten auch

von Kriminellen für ihre Zwecke eingesetzt werden. Der Gesetzgeber hat in dieser Konfliktlage entschieden, dem Interesse an Strafverfolgung und Notsuche den Vorrang zu geben.

30. Der Schwere des Grundrechtseingriffs trägt der Gesetzgeber Rechnung, indem er mehrfache, bereits dargestellte Vorkehren gegen missbräuchliche Zugriffe auf die gespeicherten Daten getroffen hat (dringender Verdacht relativ schwerer Straftaten bzw. dringende Anhaltspunkte für schwere Gefährdung von Gesundheit oder Leben; Subsidiarität; Anordnungs- und Genehmigungsverfahren; Schutz von Berufsgeheimnissen). Erwähnung verdient auch die gesetzliche Verpflichtung der Fernmeldedienstanbieterinnen, verschiedene Massnahmen zur Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu ergreifen (Art. 7 DSG und Art. 8–11 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz, VDSG, SR 235.11). Das Risiko staatlichen Machtmissbrauchs wird durch die Speicherung der Daten bei den privaten Fernmeldedienstanbieterinnen reduziert.

31. Diese Lösung erlaubt es, die zu wahrenden öffentlichen und privaten Interessen schwerer zu gewichten als den Eingriff in das Grundrecht der von der Vorratsdatenspeicherung betroffenen Personen.

32. Die **Europäische Menschenrechtskonvention** (EMRK, SR 0.101) schützt in ihrem Artikel 8 Absatz 1 das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Das systematische Sammeln und Speichern von Daten bestimmter Personen durch Sicherheitsdienste stellt auch ohne Anwendung heimlicher Überwachungsmethoden einen Eingriff in das Privatleben dieser Personen dar (EGMR-Urteil *Rotaru c. Roumanie* [Grande Chambre], ACEDH 2000-V, S. 61 ff., §§ 43 f.). Die Bestimmung schützt auch das Fernmeldegeheimnis (vgl. EGMR-Urteil *Kennedy c. Royaume-Uni* vom 18. Mai 2010, Beschwerde-Nr. 26839/05, § 118-129; Elisabet Fura/Mark Klammberg, The chilling effect of counter-terrorism measures: A comparative analysis of electronic surveillance laws in Europe and the USA, in: Freedom of Expression - Essays in honour of Nicolas Bratza, Oisterwijk 2012, S. 463 ff., 470 f. [m.w.H.]). Die Geolokalisation einer Person beispielsweise gilt als Eingriff in deren Privatleben (Urteil *Uzun gegen Deutschland* vom 2. September 2010 [deutsche Übersetzung], Beschwerde-Nr. 35623/05, § 52).

33. Eingriffe in den Schutzbereich von Artikel 8 Absatz 1 EMRK sind nach dessen Absatz 2 nur zulässig, wenn sie gesetzlich vorgesehen und zur Erreichung eines der ausdrücklich genannten Schrankenziele (u.a. öffentliche Sicherheit, Verhütung von Straftaten, Schutz der Rechte und Freiheiten anderer) in einer demokratischen Gesellschaft notwendig sind. Bei geheimen Massnahmen zur Überwachung von Kommunikationsdiensten im Rahmen von Strafverfahren oder durch Geheimdienste muss das Gesetz hinreichend klar und für die Bürger in angemessener Weise erkennbar darlegen, unter welchen Bedingungen und Umständen die Behörden befugt sind, auf solche Massnahmen zurückzugreifen (EGMR-Urteil *Kennedy c. Royaume-Uni* vom 18. Mai 2010, Beschwerde-Nr. 26839/05, § 152 f.). Die Anforderungen an die Bestimmtheit hängen von verschiedenen Faktoren ab, etwa dem Inhalt des Normtexts, dem Anwendungsbereich oder den Adressaten (EGMR-Urteil *M.K. c. France* vom 18. April 2013, Beschwerde-Nr. 19522/09, § 30). Der Europäische Gerichtshof für Menschenrechte (EGMR) leitet zudem aus dem in der Präambel der EMRK verankerten Rechtsstaatsprinzip einen gewissen Schutz gegenüber willkürlichen staatlichen Eingriffen in die Konventionsrechte ab (Urteil *Uzun gegen Deutschland* vom 2. September 2010 [deutsche Übersetzung], Beschwerde-Nr. 35623/05, § 63); der Sache nach geht es um einen "Schutz durch das Verfahren" (Jochen Abr. Frowein/Wolfgang Peukert, EMRK-Kommentar, 3. Auflage 2008,

Kehl/Strassburg/Arlington 2009, Vorbemerkung zu Art.8-11, N5 f.). Der Begriff "notwendig" in Artikel 8 Absatz 2 bedeutet weder "unbedingt erforderlich" noch "zulässig", "nützlich" oder "vernünftig", sondern dass der Eingriff einem dringenden sozialen Bedürfnis ("besoin social impérieux") zu entsprechen hat (vgl. statt vieler EGMR-Urteil *Handyside c. Royaume-Uni* vom 7. Dezember 1976, série A, volume 24, § 48). Erhöhte Anforderderungen an die Notwendigkeit des Eingriffs gelten, wenn die fraglichen Daten automatisiert bearbeitet werden. Erforderlich sind diesfalls insbesondere Vorkehren, die sicherstellen dass die Dauer der Aufbewahrung auf das Unerlässliche beschränkt wird und die erhobenen Daten vor unangemessener oder missbräuchlicher Verwendung wirksam geschützt sind (EGMR-Urteil *M.K. c. France* vom 18. April 2013, Beschwerde-Nr. 19522/09, § 35). Auch der EGMR nimmt mithin eine Prüfung der Verhältnismässigkeit vor.

34. Für das Vorliegen eines Eingriffs in den Schutzbereich von Artikel 8 EMRK und für seine Rechtfertigung kann nach dem Gesagten auf die obenstehenden Ausführungen zur Verfassungsmässigkeit verwiesen werden.

35. Insgesamt betrachtet erscheint der Eingriff in den Schutzbereich des Grundrechts des Fernmeldegeheimnisses als gerechtfertigt.

Meinungsfreiheit

36. Zur Meinungsfreiheit argumentiert der Gesuchsteller, die Vorratsdatenspeicherung sei geeignet, das Kommunikationsverhalten der betroffenen Personen nachhaltig zu beeinflussen und sie in ihrer Nutzung der betroffenen Kommunikationstechnologien zu beeinträchtigen («chilling effect»; Gesuch Ziff. II.B.9, 37 und 38). Tatsächlich ist zuzugestehen, dass die Möglichkeit der rückwirkenden Überwachung ein diffuses Gefühl des Beobachtetseins auslösen oder verstärken kann. Dies ist als mittelbarer Eingriff in den Schutzbereich der Meinungsfreiheit (Art. 16 Abs. 1 und 2 BV, Art. 10 EMRK) zu werten (vgl. Müller/Schefer S. 375–377). Zu beachten ist allerdings, dass der «chilling effect» durch die verschiedenen oben dargestellten gesetzgeberischen Sicherungsmassregeln abgemildert wird (Speicherung nur von Randdaten, gesetzliche Voraussetzungen sowie hohe verfahrensrechtliche Hürden für den Zugriff usw.).

37. Die gesetzlichen Grundlagen, die im Spiel stehenden Interessen sowie das Verhältnis zwischen ihnen unterscheiden sich in Bezug auf die Meinungsfreiheit nicht von dem, was zum Fernmeldegeheimnis gesagt wurde. Der Grundrechtseingriff ist daher ebenfalls als gerechtfertigt zu betrachten.

Unschuldsvermutung

38. Der Gesuchsteller rügt eine Verletzung der Unschuldsvermutung (Gesuch Ziff. II.B.5 und 29–32). Er argumentiert, die Vorratsdatenspeicherung erlaube es den Behörden, einen nicht vorbestehenden Tatverdacht gegen eine bestimmte Person durch die Überwachung erst zu generieren; dadurch werde auch Artikel 197 Absatz 1 Buchstabe b StPO nicht respektiert.

39. Diese Argumentation geht fehl. Weder die Unschuldsvermutung als Grundrecht nach Artikel 197 StPO verlangt, dass die Strafverfolgungsbehörden bei der Anordnung von Zwangsmassnahmen die Identität der Person, gegen die sich der Verdacht richtet, bereits kennen. Vielmehr genügt bei Fahndungen gegen Unbekannt die Individualisierbarkeit der Zielpersonen (BGE 137 IV 340 E. 5.6). Es trifft zu, dass die unter die Speicherpflicht fallenden Randdaten auch Fahndungsmethoden erlauben würden, bei denen ohne vorbestehenden Tatverdacht nach möglichen Delikten «gefischt»

wird. Dies verhindert der Gesetzgeber aber, indem er für die Übermittlung von Randdaten an eine Strafverfolgungsbehörde – neben den anderen Voraussetzungen – das Vorliegen eines dringenden Tatverdachts voraussetzt. Die geltende Regelung stellt demnach sicher, wie dies auch der EGMR in seiner Rechtsprechung postuliert (EGMR-Urteil M.K. c. France vom 18. April 2013, Beschwerde-Nr. 19522/09, § 36), dass der Gesuchsteller oder andere Betroffene nicht allein infolge der Speicherung ihrer Randdaten dem Vorwurf eines strafbaren Verhaltens ausgesetzt sind.

40. Auch losgelöst von dieser spezifischen Thematik ist nicht ersichtlich, inwiefern die Unschuldsvermutung verletzt sein soll.

Datenschutzrecht

41. Laut dem Gesuch (Ziff. II.B.21) verletzt die Vorratsdatenspeicherung den datenschutzrechtlichen Grundsatz der Zweckbindung (Art. 4 Abs. 4 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1). Dabei übersieht der Gesuchsteller, dass Daten laut dieser Bestimmung nicht nur für Zwecke bearbeitet werden dürfen, die bei der Beschaffung angegeben wurden oder aus den Umständen ersichtlich sind, sondern auch für Zwecke, die gesetzlich vorgesehen sind. Die gesetzlichen Grundlagen der Vorratsdatenspeicherung sowie der Herausgabe der Daten an Behörden wurden im Zusammenhang mit dem Fernmeldegeheimnis dargestellt.

42. Was die Verhältnismässigkeit der Datenbearbeitung (Gesuch Ziff. II.B.21) angeht, kann ebenfalls auf die Ausführungen zum Fernmeldegeheimnis verwiesen werden (Ziff. 24–29).

43. Auch die Kritik des Gesuchstellers an den rechtlichen Vorgaben zur Datensicherheit (Gesuch Ziff. II.B.24) trifft nicht zu. Es ist richtig, dass die Gesetzgebung den Fernmeldedienstanbieterinnen keine konkreten Datensicherheitsmassnahmen im technischen Detail vorschreibt. Artikel 7 DSG und die Artikel 8–11 VDSG verpflichten die Anbieterinnen hingegen in technologieneutraler Sprache, verschiedene Massnahmen zur Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu ergreifen. Angesichts des schnellen Wandels der Technik wäre es nicht sinnvoll, den Anbietern genauere Vorgaben zu machen.

44. Aus den vorstehenden Erwägungen ergibt sich, dass die Vorratsdatenspeicherung durch die Fernmeldedienstanbieterin X zulässig ist. Demzufolge ist das Begehren 1 abzuweisen.

Verfahrens- und Parteikosten

45. Das BÜPF und die Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF, SR 780.115.1) regeln die Verfahrenskosten für Verfügungen wie die vorliegende nicht. Daher ist eine Gebühr nach Artikel 13 Absatz 2 der Verordnung vom 10. September 1969 über Kosten und Entschädigungen im Verwaltungsverfahren (SR 172.041.0) zu erheben. Der Umfang des Gesuchs und die Komplexität der aufgeworfenen Rechtsfragen haben einigen Verwaltungsaufwand ausgelöst. Angesichts der Zahl von sechs ungefähr gleichlautenden Gesuchen rechtfertigt sich eine entsprechende Reduktion des Betrags. Die Gebühr ist innerhalb des Rahmens von 200–7000 Franken (Absatz 2 Buchstabe a Ziffer 2) daher auf 500 Franken festzulegen.

46. Eine Parteientschädigung ist im ersteinstanzlichen Verwaltungsverfahren nicht vorgesehen und wäre angesichts des Ausgangs des Verfahrens ohnehin nicht zuzusprechen.

Aufgrund dieser Erwägungen wird verfügt:

1. Auf das Begehren 2 (Herausgabe von Daten an Behörden unterlassen) wird nicht eingetreten.
2. Im Übrigen wird das Gesuch abgewiesen.
3. Die Verfahrenskosten in der Höhe von 500 Franken werden dem Gesuchsteller auferlegt.
4. Eine Parteientschädigung wird nicht zugesprochen.

Rechtsmittelbelehrung:

Gegen diese Verfügung kann innerhalb von 30 Tagen nach Eröffnung gemäss Art. 44 ff. VwVG und Art. 31 ff. des Bundesgesetzes vom 17. Juni 2005 über das Bundesverwaltungsgericht (VGG; SR 173.32) Beschwerde erhoben werden.

Die Beschwerde ist schriftlich und im Doppel direkt beim Bundesverwaltungsgericht, Postfach, 9023 St. Gallen einzureichen. Sie hat die Begehren, deren Begründung mit Angabe der Beweismittel sowie die Unterschrift der Beschwerdeführenden oder ihrer Vertretung zu enthalten. Die angefochtene Verfügung sowie allfällige weitere als Beweismittel angerufene Urkunden sind beizulegen, soweit die Beschwerdeführende sie in Händen hat. Eine allfällige Vertretung kann aufgefordert werden, sich durch schriftliche Vollmacht auszuweisen.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Informatik Service Center ISC-EJPD
Überwachung Post- und Fernmeldeverkehr ÜPF

René Koch
Leiter Dienst ÜPF

Zu eröffnen mit
eingeschriebenem Brief:
Vorname Name des Adressaten
Strasse Nummer
Postleitzahl Ort

Kopie an:
Fernmeldedienstanbieterin X
Strasse Nummer
Postleitzahl Ort