Erläuternder Bericht Entwurf März 2017

zur Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11)

A. Ausgangslage

Die Totalrevision des Bundesgesetzes vom 6. Oktober 2000[1] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) bedingt eine Totalrevision seiner Ausführungsverordnungen, so unter anderem auch der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF).

Der Aufbau der vorliegenden Verordnung folgt der Trennung zwischen allgemeinen Bestimmungen, Postverkehr, Fernmeldeverkehr und Schlussbestimmungen. Der Wunsch nach mehr Rechtssicherheit führte dazu, dass die aktuelle VÜPF die einzelnen Rechte und Pflichten sehr detailliert beschreibt. So wird in der Verordnung zum Beispiel nicht mehr lediglich zwischen Echtzeit- und rückwirkenden Überwachungstypen unterschieden, sondern die Verordnung ist so aufgebaut, dass es für jeden angebotenen Dienst eigenständige Bestimmungen gibt, welche jeweils - soweit zutreffend - dessen Überwachung in Echtzeit sowie rückwirkend beschreiben. Dies führt dazu, dass auch die einzelnen Voraussetzungen eines Auskunfts- beziehungsweise Überwachungstyps sehr detailliert beschrieben sind.

Durch die hohe Regelungsdichte wird nebst der erwünschten Rechtssicherheit das Ziel verfolgt, im Bereich des Fernmeldeverkehrs eine höchstmögliche Standardisierung bei den Auskunfts- und Überwachungstypen zu erreichen und damit die automatischen Abläufe zu begünstigen.

Ein weiterer Unterschied zur bisherigen Verordnung bildet des Weiteren der Umstand, dass in der aktuellen Verordnung nicht mehr zwischen leitungsvermittelten (CS) und paketvermittelten (PS) Fernmeldediensten differenziert wird. Eine solche Differenzierung ist aufgrund des Technologiewechsels nicht mehr zeitgemäss. So wird zum Beispiel vermehrt über das Internet telefoniert. Neu werden hingegen die einzelnen Überwachungstypen aufgeteilt in Überwachungen von Netzzugangsdiensten (8. Abschnitt und Art. 60) und Überwachungen von Anwendungen (9. Abschnitt und Art. 61–63).

Im Rahmen der Totalrevision des Bundesgesetzes wurde zudem der Kreis der Mitwirkungspflichtigen erweitert. So war es beispielsweise nach der bisherigen Gesetzgebung nicht möglich, den nicht meldepflichtigen Fernmeldedienst-anbieterinnen und solchen Anbieterinnen, die ihre Kommunikationsdienste über das Internet anbieten, ohne Internetzugangsanbieterin zu sein, die Pflichten im Bereich der Überwachung zu überbinden. Nach der Totalrevision sind im Artikel 2 Buchstabe c BÜPF nun auch Anbieterinnen abgeleiteter Kommunikationsdienste vom persönlichen Geltungsbereich erfasst. Bei den Anbieterinnen abgeleiteter Kommunikationsdienste handelt es sich um solche Anbieterinnen, deren Dienste

[1] SR **780.1**

sich auf Fernmeldedienste stützen und die ihren Benutzerinnen und Benutzern eine Einweg- (z. B. Hochladen eines Dokumentes) oder Mehrwegkommunikation (z. B. E-Mail, Instant Messaging oder Chatdienst) ermöglichen. Neu ist zudem, dass der persönliche Geltungsbereich im Bereich der Fernmeldeüberwachung nicht mehr an die vom Fernmeldegesetz[2] in Artikel 4 vorgeschriebene Meldepflicht geknüpft wird. Damit sind auch solche Anbieterinnen vom persönlichen Geltungsbereich erfasst, die nach bisherigem Recht nicht meldepflichtig waren.

Ausgehend von dieser Regelung könnte erwartet werden, dass auch die Anzahl der Mitwirkungspflichtigen zunimmt, die Auskunfts- und Überwachungspflichten aktiv auszuführen hätten. Die Zahl solcher Mitwirkungspflichtigen wird jedoch höchstwahrscheinlich abnehmen. Dies deshalb, weil das Gesetz neu dem Bundesrat auch die Möglichkeit einräumt, Anbieterinnen von Fernmeldediensten von gewissen Überwachungspflichten auszunehmen, wenn diese Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten (siehe Erläuterungen zu Art. 49). Den Anbieterinnen abgeleiteter Kommunikationsdienste, die eine Überwachung grundsätzlich zu dulden haben, können hingegen weitergehende Auskunfts- und Überwachungspflichten auferlegt werden, wenn sie Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten. Da die Voraussetzungen sehr streng sind, werden zahlenmässig jedoch nicht sehr viele Anbieterinnen abgeleiteter Kommunikationsdienste eine Überwachung aktiv auszuführen haben (siehe Ausführungen zu Art. 50) und sehr viele Fernmeldedienstanbieterinnen, die bisher diese Pflicht hatten, haben sie nun nicht mehr. Die meisten Anbieterinnen abgeleiteter Kommunikationsdienste und Fernmeldedienstanbieterinnen werden lediglich allfällige Überwachungen zu dulden haben, die durch den Dienst ÜPF oder durch von diesem beauftragte Personen durchgeführt werden. Zu diesem Zweck müssen sie unverzüglich Zugang zu ihren Anlagen gewähren. Ausserdem müssen sie die für die Durchführung der Überwachung notwendigen Informationen liefern, die von ihnen angebrachten Verschlüsselungen entfernen und die ihnen zur Verfügung stehenden Randdaten liefern (zum Begriff Randdaten siehe die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels). Des Weiteren wurde durch die Totalrevision gewissen Bundesstellen ausdrücklich die Möglichkeit eingeräumt, beim Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ein Auskunftsgesuch zu stellen beziehungsweise einen Überwachungsauftrag einzureichen (siehe Ausführungen zu Art. 1). So kann neu das Staatssekretariat für Wirtschaft ihr Strafantragsrecht einfacher wahrnehmen und unerwünschte Werbeanrufe effektiv bekämpfen, da es aufgrund der neuen Regelung beim Dienst ÜPF Auskünfte über den betreffenden Fernmeldeanschluss verlangen kann. Und der Nachrichtendienst des Bundes kann nun ebenfalls alle Auskunftstypen beim Dienst ÜPF einholen.

Neu soll auch die Qualität der übermittelten Auskunfts- und Überwachungsdaten überprüft werden können, damit der reibungslose Ablauf der Überwachungen nicht beeinträchtigt wird. Die Verordnung legt fest, wann die erforderliche Qualität gewahrt ist und wer die erforderliche Qualität sicherzustellen hat (siehe Ausführungen zu Art. 27. Der Dienst ÜPF nimmt dabei die Funktion einer Aufsichtsbehörde wahr und kann bei Nichtbeachtung der gesetzlichen Bestimmungen, beispielsweise der Qualitätsbestimmung, die betreffenden

[2] SR **784.2**

Anbieterinnen nach den Vorgaben von Artikel 41 BÜPF oder von Artikel 39 Absatz 1 Buchstabe a BÜPF verwaltungsrechtlich beziehungsweise sogar strafrechtlich sanktionieren.

Um die ordnungsgemässe Ausführung der angeordneten Überwachungen des Fernmeldeverkehrs und die Erteilung von Auskünften sicherzustellen, wird des Weiteren das vom Dienst ÜPF bereits angewandte sogenannte Compliance-Verfahren gesetzlich verankert. Es handelt sich hierbei um das Verfahren zur Überprüfung der Auskunfts- und Überwachungsbereitschaft einer Anbieterin (Art. 31–34 BÜPF). Dabei wird überprüft, ob eine auskunfts- beziehungsweise überwachungspflichtige Anbieterin in der Lage ist, nach dem anwendbaren Recht Auskünfte zu erteilen beziehungsweise Überwachungen durchzuführen (siehe Ausführungen zu Art. 29–32).

B. Erläuterungen zu den einzelnen Artikeln

1. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Einleitung

Art. 1 Gegenstand und Geltungsbereich

Artikel 1 Absatz 1 entspricht dem bisherigen Artikel 1 Absatz 1 VÜPF vom 31. Oktober 2001[3] (Stand 1. Januar 2012).

Absatz 2 präzisiert den persönlichen Geltungsbereich von Artikel 2 BÜPF. Aufgeführt werden wie im bisherigen Artikel 1 VÜPF als Adressaten die anordnenden und die verfahrensleitenden Behörden (in der Regel die Staatsanwaltschaften; *Bst. a*) und die Genehmigungsbehörden (in der Regel die Zwangsmassnahmengerichte; *Bst. b*). Die Polizeibehörden des Bundes, der Kantone und Gemeinden (*Bst. c)* wurden neu eingefügt, um eine abschliessende Liste aller auskunftsberechtigten Stellen aufführen zu können. Die Aufzählung der Adressaten wurde gegenüber der VÜPF vom 31. Oktober 2001[4] aufgrund der Bestimmungen des Artikels 15 Absatz 2 Buchstaben a und b BÜPF um den Nachrichtendienst des Bundes (NDB; *Bst. d*) und das Staatssekretariat für Wirtschaft (SECO; *Bst. e*) auf Seiten der auskunftsberechtigten Stellen ergänzt. Hinzu kommen die in Artikel 15 Absatz 1 Buchstabe c BÜPF aufgeführten Behörden des Bundes und der Kantone zwecks Erledigung von Verwaltungsstrafsachen (*Bst. f*). Und schliesslich fällt auch der Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF; *Bst. g*) selbstverständlich in den Geltungsbereich der VÜPF.

Eine der wichtigsten Änderungen der Totalrevision des BÜPF besteht in der Erweiterung des Kreises der sogenannten **Mitwirkungspflichtigen**. Damit sind diejenigen Personen gemeint, die dem BÜPF unterstellt sind und denen daraus Pflichten erwachsen, seien es aktive Pflichten, wie die sogenannte Überwachungsbereitschaft (siehe Art. 32 BÜPF) oder passive Pflichten, wie die Duldungspflicht (siehe Art. 26 Abs. 2 und 6, 27 Abs. 1 und 2, 28 und 29 BÜPF). Die Kategorien von Mitwirkungspflichtigen werden in Absatz 2 Buchstabe h–m wie folgt aufgeführt:

- *Buchstabe h*: Die Anbieterinnen von Postdiensten (PDA) nach dem Postgesetz vom 17. Dezember 2010[5] (PG)[6];

- *Buchstabe i*: Die Anbieterinnen von Fernmeldediensten (FDA) nach Artikel 3 Buchstabe b des Fernmeldegesetzes vom 30. April 1997[5] (FMG)[7];

3 SR **780.11**
4 SR **780.11**
5 SR **783.0**
6 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. a, BBl **2013** 2706 in fine.
7 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. b, BBl **2013** 2707.

- *Buchstabe j*: Die Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste)[8];

- *Buchstabe k*: Die Betreiberinnen von internen Fernmeldenetzen[9];

- *Buchstabe l*: Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen[10];

- *Buchstabe m:* Professionelle Wiederverkäuferinnen von Karten und ähnlichen Mitteln, die den Zugang zu einem öffentlichen Fernmeldenetz ermöglichen[11].

Art. 2 Begriffe und Abkürzungen

Artikel 2 orientiert sich an Artikel 2 der VÜPF vom 31. Oktober 2001[12] und führt die Definition der zahlreichen Begriffe und Abkürzungen in einem Anhang auf.

2. Abschnitt: Überwachungsanordnung

Art. 3 Eingaben beim Dienst ÜPF

Artikel 3 Absatz 1 befasst sich mit den zugelassenen Übertragungsmitteln für die Einreichung der Überwachungsanordnungen sowie deren Verlängerung und Aufhebung und die Mitteilung der einzurichtenden Zugriffsrechte von den anordnenden Behörden an den Dienst ÜPF.

Die Zugriffsrechte im Verarbeitungssystem des Dienstes ÜPF gelten für die jeweils angeordnete Überwachungsmassnahme und beziehen sich auf die durch die jeweilige anordnende Behörde bezeichneten Mitglieder der Strafverfolgungsbehörden, die mit dem jeweiligen Fall befasst sind und diese Daten im Rahmen der Strafermittlung bearbeiten müssen. Die Zugriffsrechte werden in der Regel zweistufig verwaltet. Jede an Überwachungsmassnahmen beteiligte Strafverfolgungsbehörde bestimmt in der Regel eine für die Verwaltung ihrer Benutzerschaft zuständige Person mit der Funktion Organisationsadministrator (OrgAdmin), welche die Zugriffsrechte innerhalb der Behörde pro Überwachungsmassnahme verwaltet. Der Dienst ÜPF berechtigt die jeweiligen OrgAdmin auf die Überwachungsmassnahme gemäss den Angaben der anordnenden Behörde in der Überwachungsanordnung (siehe Art. 47). Der dadurch berechtigte OrgAdmin der Strafverfolgungsbehörde verwaltet dann selbständig die Zugriffsrechte auf die einzelnen Überwachungen für die Mitglieder seiner Behörde im Verarbeitungssystem gemäss den Angaben der anordnenden Behörde (vgl. dazu Art. 8 und 9 der Verordnung vom xx.xx.xxxx[13] über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs [VVS-ÜPF]).

8 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. c, BBl **2013** 2707 in fine.
9 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. d, BBl **2013** 2708 in fine.
10 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. e, BBl **2013** 2709.
11 Siehe Botschaft vom 27. Februar 2013 zum BÜPF, zum Art. 2 Bst. f, BBl **2013** 2709.
12 SR **780.11**
13 SR **XX.XXX**

Alternativ kann eine Strafverfolgungsbehörde die Benutzerverwaltung pro Überwachungsmassnahme auch als Dienstleistung des Dienstes ÜPF beziehen. Der Dienst ÜPF verwaltet in diesem Fall die Zugriffsrechte der einzelnen Benutzenden der jeweiligen Strafverfolgungsbehörde auf die Überwachungsmassnahme gemäss den Angaben der anordnenden Behörde in der Überwachungsanordnung (siehe Art. 47).

Falls Änderungen erforderlich sind, welche die Überwachungsmassnahme betreffen (z. B. Änderung oder Hinzufügen eines Überwachungstyps, Änderung des überwachten Adressierungselements aufgrund von Flüchtigkeitsfehlern bei den Strafverfolgungsbehörden), muss die anordnende Behörde eine neue gebührenpflichtige Überwachungsanordnung beim Dienst ÜPF einreichen. Änderungen von Zugriffsrechten lösen keine neue Gebühr aus.

Zu den nach *Buchstabe a* "durch den Dienst ÜPF zugelassenen sicheren Übertragungsmitteln" zählt zum Beispiel eine elektronische Auftragsschnittstelle gemäss ETSI-Standards wie auch die vom Dienst ÜPF genutzten Verschlüsselungslösungen für E-Mails. Die entsprechenden Vorschriften erlässt das Departement in der VD-ÜPF (siehe auch die Erläuterungen zu Art. 70).

Buchstabe b erlaubt eine Übermittlung der genannten Dokumente per Post oder Telefax an den Dienst ÜPF. Diese Übermittlung ist jedoch nur erlaubt, falls technische Gründe eine Übermittlung gemäss Buchstabe a verhindern. Die Strafverfolgungsbehörden haben die Dokumente also primär nach Buchstabe a dem Dienst ÜPF zu zustellen und haben alles daran zu setzen, dass sie dazu in der Lage sind.

Buchstabe c hält fest, dass nach einer telefonischen Anordnung, welche nur in dringlichen Fällen (z. B. Notsuchen, Fahndungen, Anordnungen ausserhalb der Normalarbeitszeiten) zulässig ist, die Anordnung mit einem Übertragungsmittel gemäss Buchstabe a oder b nachgereicht werden muss.

Nach *Absatz 2* sollen die Übertragungsmittel nach Absatz 1 Buchstabe a durch einen Online-Zugriff auf das Verarbeitungssystem des Dienstes ersetzt werden. Dies vereinfacht den anordnenden Behörden die Eingaben beim Dienst ÜPF erheblich, weshalb der Zeitpunkt durch diesen bestimmt werden soll, ab welchem die Eingaben nur noch über den Online-Zugriff eingereicht werden.

Art. 4 Durchführung der Überwachung

Artikel 4 entspricht im Wesentlichen dem Artikel 17 Absatz 1 und 6 der VÜPF vom 31. Oktober 2001[14] und regelt die Durchführung der Überwachung.

Absatz 1 entspricht der bisherigen Regelung.

Sollte die Mitwirkungspflichtige auf Grund betrieblicher Probleme nicht in der Lage sein, ihre Pflichten zur Überwachung des Post- und Fernmeldeverkehrs wahrzunehmen, muss sie dies gemäss *Absatz 2* neu dem Dienst ÜPF nicht nur unverzüglich melden, sondern hat zusätzlich eine schriftliche Begründung nachzuliefern. Betriebliche Probleme schliessen sowohl technische, als auch organisatorische Gründe ein. Diese Probleme können Konsequenzen haben (z.B. Art. 33 Abs. 5 und Art. 34 Abs. 1 BÜPF).

14 SR **780.11**

Es ist wichtig, dass die Mitwirkungspflichtige unverzüglich den Dienst ÜPF über alle Probleme informiert, welche die zeitkritischen Überwachungen bzw. Überwachungsaufträge betreffen. Daher hat diese Meldung sofort telefonisch an die entsprechenden Kontaktstellen des Dienstes ÜPF zu erfolgen. Falls die Mitwirkungspflichtige nicht in der Lage sein sollte, einen Überwachungsauftrag auszuführen oder ihre Pflichten bei der Durchführung von Echtzeitüberwachungen zu erfüllen, hat sie den zuständigen Bereich des Dienstes ÜPF innerhalb der Bürozeiten über dessen zentrale Telefonnummer bzw. ausserhalb der Bürozeiten über dessen Pikettnummer zu kontaktieren. Die Mitwirkungspflichtige hat dem Dienst ÜPF die Störungsmeldung in schriftlicher Form unter Angabe des genauen Ausfallzeitraums, der Problembeschreibung, einer chronologischen Übersicht der eingeleiteten Massnahmen und des Problemstatus am nächsten Arbeitstag zukommen zu lassen. Falls die Störung zu diesem Zeitpunkt noch nicht behoben ist, hat sie ausserdem dem Dienst ÜPF nach der Störungsbehebung eine gleichartige schriftliche Abschlussmeldung zu senden.

Im Falle solcher Störungen und unabhängig davon, auf welcher Seite die Probleme aufgetreten sind, hat die Mitwirkungspflichtige nach *Absatz 3* mindestens die Randdaten der Echtzeitüberwachung während der in den technischen Vorschriften des EJPD angegebenen Zeitspanne zwischenzuspeichern und unverzüglich nachzuliefern (zum Begriff *Randdaten der Echtzeitüberwachung* siehe die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels). Falls die Randdaten der Echtzeitüberwachung nicht mehr verfügbar oder unvollständig sein sollten, hat die Mitwirkungspflichtige gemäss den Anweisungen des Dienstes ÜPF unverzüglich die entsprechenden Randdaten der rückwirkenden Überwachung zu liefern (zum Begriff *Randdaten der rückwirkenden Überwachung* siehe die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels).

Art. 5 Schutz von Amts- und Berufsgeheimnissen

Artikel 5 entspricht den Artikeln 17 Absatz 2 (Überwachung der Telefondienste) und 25 Absatz 2 (Überwachung des Internets) VÜPF vom 31. Oktober 2001[15] und hat den Schutz des Amts- und Berufsgeheimnisses zum Ziel. Diese Bestimmung regelt nur die Situation, wenn der Dienst ÜPF feststellt, dass die Überwachung einen Amts- oder Berufsgeheimnisträger betrifft, ohne dass Vorkehren gemäss Art. 271 StPO bzw. Art. 70*b* MStP getroffen worden sind (*Buchstaben a und b*).

Gemäss Artikel 16 Buchstabe e BÜPF setzt der Dienst ÜPF die von der Genehmigungsbehörde angeordneten Vorkehren zum Schutz von Amts- und Berufsgeheimnissen um. "Diese Aufgabe wird auf die Überwachung des Postverkehrs ausgeweitet, da sie auch in diesem Bereich durchaus sinnvoll ist. Diese Bestimmung muss zu den Artikeln 271 und 274 Absatz 4 Buchstabe a StPO sowie zu den Artikeln 70*b* und 70*e* Absatz 4 Buchstabe a MStP in Beziehung gesetzt werden. In diesen Artikeln wird die auf die Überwachung anwendbare Regelung erwähnt, falls ein Amts- oder Berufsgeheimnis geschützt werden muss, von dem die Strafverfolgungsbehörde keine Kenntnis erhalten darf. Der Dienst trifft die notwendigen Vorkehren für die Umsetzung der Massnahmen, die im Rahmen der oben aufgeführten Artikel beschlossen wurden; er nimmt aber zum

15 SR **780.11**

Beispiel nicht selbst die Aussonderung vor, die in diesen Artikeln erwähnt ist (Art. 271 StPO und Art. 70*b* MStP)"[16].

Nach Artikel 15 Buchstabe j und k (Postverkehr) beziehungsweise nach Artikel 47 Buchstabe k und l (Fernmeldeverkehr) muss die beim Dienst ÜPF eingereichte Überwachungsanordnung den Vermerk betreffend die Personen, die einem Amts- oder Berufsgeheimnis gemäss Artikel 271 StPO oder gemäss Artikel 70b MStP unterstehen, sowie die Vorkehrungen zu deren Schutz, enthalten; siehe auch Artikel 9 Absatz 2 Buchstabe i, wonach die Überwachungsakte aus den besonderen angeordneten Schutzmassnahmen bestehen.

Gemäss BÜPF kann der Dienst ÜPF die ihm übermittelten Überwachungsanordnungen nicht nur einer formellen Prüfung, sondern auch einer materiellen Prüfung unter dem Gesichtspunkt des Verwaltungsrechts, unterziehen[17]. Im Rahmen dieser Prüfung könnte der Dienst ÜPF eine entsprechende Feststellung machen, so z.B. wenn die Berufsbezeichnung einen Hinweis auf einen entsprechenden Beruf macht und keine Triage verfügt wurde.

Soll beispielsweise ein Arzt überwacht werden, welcher dem Arztgeheimnis untersteht, ohne dass Vorkehrungen gemäss Artikel 271 StPO oder gemäss Artikel 70b MStP angeordnet worden sind, so wird die Überwachung zwar durch den Dienst ÜPF ausgeführt, die anordnende Behörde erhält jedoch vorerst keinen Zugriff auf die aufgezeichneten Daten. Die anordnende Behörde sowie die Genehmigungsbehörde werden entsprechend darüber orientiert. Die Genehmigungsbehörde hat die Möglichkeit die Überwachung unter Auflage einer Triage gemäss Artikel 271 Absatz 1 und 274 Absatz 4 Buchstabe a StPO oder gemäss Artikel 70b und 70e Absatz 4 Buchstabe a MStP zu genehmigen. Sie kann einen Verantwortlichen ernennen, welcher die Daten vorgängig sichtet und eine entsprechende Triage vornimmt. Wird ein Verantwortlicher ernannt, wird diesem durch den Dienst ÜPF die Berechtigung und/oder der Zugriff auf die entsprechenden Daten im Verarbeitungssystem erteilt. Dem Dienst ÜPF wird dann durch die Genehmigungsbehörde mitgeteilt, auf welche Daten die anordnende Behörde Zugriff erhalten soll. Wurde eine Triage angeordnet, so erhält der Dienst ÜPF von der Genehmigungsbehörde regelmässig eine entsprechende Liste und nimmt die Triage im Verarbeitungssystem vor. Das heisst, die anordnende Behörde erhält auf die von der Genehmigungsbehörde ausgewählten Daten Zugriff und die restlichen Daten werden durch den Dienst ÜPF vernichtet[18]. Dieser Vorgang gilt für die gesamte Überwachungsdauer.

Buchstabe c hält fest, dass das Vorerwähnte für den Nachrichtendienst des Bundes (NDB) als anordnende Behörde sinngemäss gilt. In diesem Fall ist die Genehmigungsbehörde das Bundesverwaltungsgericht.

Art. 6 Geheimhaltungspflicht

Artikel 6 entspricht dem Artikel 17 Absatz 7 und Artikel 25 Absatz 7 VÜPF vom 31. Oktober 2001[19] und regelt die Geheimhaltungspflicht.

16 BBl **2013** 2725 in fine und 2726 in initio; siehe auch die Erläuterungen in der Botschaft zum BÜPF zu Art. 271 StPO und 70*b* MStP.
17 BBl **2013** 2696; Ziff. 1.4.5.
18 BBl **2006** 1249
19 SR **780.11**

Die Geheimhaltungspflicht ist insbesondere für den Erfolg der Überwachungsmassnahmen und Auskünfte sowie für den Schutz der Persönlichkeitsrechte der betroffenen Personen von besonderer Wichtigkeit und darf keinesfalls in irgendeiner Weise verletzt werden. Weder die betroffene Person noch unbefugte Dritte dürfen direkt oder indirekt Hinweise über Überwachungen oder Auskunftserteilungen erhalten (siehe auch Art. 320 StGB und Art. 39 Abs. 1 Bst. d BÜPF).

Art. 7 Technische Datensortierung (Filterung)

Artikel 7 führt die Bestimmung von Artikel 17 Buchstabe g BÜPF weiter aus.

Die vorgesehene Sortierung unterscheidet sich von der Aussonderung nach Artikel 271 StPO und 70*b* MStP in Zusammenhang mit dem Schutz des Amts- und Berufsgeheimnisses (siehe oben ad Art. 5).

Unter technischer Datensortierung (Filterung) ist zu verstehen, dass die auszuwertende Datenmenge entsprechend den dokumentierten Anweisungen der anordnenden Behörde mittels automatischer Verfahren reduziert wird. Die anordnende Behörde kann die automatisierte Filterung der Überwachungsdaten verfügen, um beispielsweise die Auswertung grosser Datenmengen zu erleichtern. Dabei werden für die Ermittlungen irrelevante Daten, wie etwa Internet-TV, die keinen Erkenntnisgewinn für die Strafbehörden darstellen, bereits vor der Speicherung im Verarbeitungssystem aus dem Datenstrom herausgefiltert, so dass sie gar nie im Verarbeitungssystem gespeichert werden.

Hiermit sind nicht die Fälle gemeint, wenn viele unbeteiligte Dritte von einer Überwachungsmassnahme betroffen sind (z.B. zentrale Telefonnummer einer Firma soll überwacht werden). Auch in solchen Fällen nimmt der Dienst ÜPF mit der anordnenden Behörde Rücksprache (sinngemäss wie in Art. 5).

Die Filterung wird durch den Dienst ÜPF kostenlos unter der Voraussetzung durchgeführt, dass sie automatisiert und mit verhältnismässigem Aufwand erfolgen kann. Unter verhältnismässigem Aufwand ist zu verstehen, dass der Dienst ÜPF im Rahmen der ihm zur Verfügung stehenden finanziellen, personellen und technischen Ressourcen die entsprechenden Vorkehrungen treffen kann. Falls der Dienst ÜPF feststellt, dass die gewünschte Filterung technisch unmöglich ist oder sie sich nicht mit verhältnismässigem Aufwand realisieren lässt, teilt er dies der anordnenden Behörde unverzüglich und begründet mit.

Die Strafverfolgungsbehörden haben die Verantwortung für die Konfiguration der vom Dienst ÜPF vorgegebenen Filtermöglichkeiten. Der Dienst ÜPF berät sie dabei. Aufgrund der hohen Anforderungen an die Durchführung dieser Filterung kommen nur automatisierte Verfahren zur Anwendung. Jede andere Art der Filterung wäre sehr kompliziert oder gar nicht realisierbar[20]. Die anordnende Behörde nimmt vor der Anordnung einer technischen Datensortierung Rücksprache mit dem Dienst ÜPF bezüglich deren Machbarkeit.

Art. 8 Aufzeichnung der Telefonate zu Beweiszwecken

Artikel 8 Absatz 1 ermöglicht dem Dienst ÜPF, zu Beweiszwecken die im Zusammenhang mit der Erfüllung seiner Aufgaben getätigten Telefonate

20 BBl **2013** 2728

aufzuzeichnen. Dies geschieht aufgrund der Tatsache, dass die anordnenden Behörden Überwachungsaufträge (zum Beispiel in dringlichen Fällen; siehe Art. 3 Abs. 1 Bst. c) beziehungsweise Erläuterungen zu Überwachungsaufträgen oft telefonisch erteilen. Vereinzelt kam es in der Vergangenheit bei nachträglichen Abklärungen zu unterschiedlichen Aussagen der Mitarbeitenden des Dienstes ÜPF und der anordnenden Behörden betreffend telefonisch in Auftrag gegebener Überwachungsmassnahmen. Im Rahmen von Untersuchungen ist es notwendig, die Fakten einwandfrei feststellen zu können. Deshalb ist es wichtig, dieses Beweisführungsmittel an der Hand zu haben.

Zudem werden bereits alle *schriftlichen* Kommunikationen zwischen Dienst ÜPF, Behörden und Mitwirkungspflichtigen aufbewahrt, z.B. Anordnungen, Verfügungen, Überwachungsaufträge, Korrespondenzen; siehe Art. 9 (Überwachungsakte). Die gleiche Regelung soll nun auch für telefonische Kommunikationen gelten.

Die Aufzeichnung der Telefonate betrifft die Büronummer und die Pikettnummer des Überwachungsmanagements des Dienstes ÜPF.

Eine allfällige Auswertung der Aufzeichnungen soll nur durch den Datenschutzbeauftragten des Dienstes ÜPF möglich sein (Abs. 2). Der Dienst ÜPF darf die Aufzeichnungen nur während zwei Jahren aufbewahren (Abs. 3). Sie sind nach Ablauf der Aufbewahrungsfrist zu vernichten.

Art. 9 Überwachungsakte

Artikel 9 beschreibt die Aktenführung des Dienstes ÜPF und führt abschliessend den Inhalt der Überwachungsakte auf.

Absatz 1 verpflichtet den Dienst ÜPF zur Anlegung einer Akte für jede Überwachungsanordnung. Diese Anordnung kann mehrere Überwachungsmassnahmen umfassen.

Absatz 2 hält fest, welche Unterlagen die Überwachungsakte umfasst. Dies sind die Überwachungsanordnung sowie allfällige Beilagen, der Überwachungsauftrag beziehungsweise die Überwachungsaufträge an die entsprechenden Mitwirkungspflichtigen, die Bestätigung beziehungsweise Bestätigungen, wann der Auftrag durch den Dienst ÜPF an die Mitwirkungspflichtigen erteilt wurde, die Quittierung (Datum und Uhrzeit) der Mitwirkungspflichtigen über die Ausführung des Überwachungsauftrags beziehungsweise der Überwachungsaufträge, die Verfügung beziehungsweise Verfügungen der Genehmigungsbehörde sowie allfällige Beschwerdeentscheide, allfällige Verlängerungsanordnungen und Verfügungen der Genehmigungsbehörde, die Aufhebungsanordnung beziehungsweise Aufhebungsanordnungen, allfällige zu der Massnahme ergangenen Korrespondenz (E-Mails etc.), allfällige besondere angeordneten Schutzmassnahmen (beispielsweise Triage) sowie die Rechnungsunterlagen.

Diese Akte bildet auch die Grundlage für die Gebührenerhebung gegenüber der anordnenden Behörde und die an die beauftragten Mitwirkungspflichtigen zu leistenden Entschädigungszahlungen.
Es besteht das Ziel, die Überwachungsakten elektronisch und nach Möglichkeit im Verarbeitungssystem aufzubewahren.
Absatz 3 regelt die Aufbewahrung der Überwachungsdaten gemäss Artikel 11 BÜPF und die Vernichtung der Überwachungsdaten gemäss Artikel 14 VVS

3. Abschnitt: Arbeitszeiten und Pikett-Regelung

Art. 10 Normalarbeitszeiten und Feiertage

Artikel 10 ist neu und definiert in *Absatz 1* die Normalarbeitszeiten. Diese entsprechen der aktuellen Praxis. Die Uhrzeiten beziehen sich auf Schweizerzeit.

Absatz 2 definiert die Feiertage. Diese entsprechen denjenigen von Artikel 66 Absatz 2 der Bundespersonalverordnung vom 3. Juli 2001[21].

Art. 11 Leistungen ausserhalb der Normalarbeitszeiten

Artikel 11 ist neu, entspricht aber der aktuellen Praxis des Dienstes ÜPF. Er regelt die Leistungen des Dienstes ÜPF sowie der Mitwirkungspflichtigen im Pikettdienst. Dringende Aufträge werden im Pikettdienst nur nach telefonischer Avisierung über die Pikettnummer des Dienstes ÜPF erledigt.

In *Absatz 1* werden die Leistungen des Dienstes ÜPF im Pikettdienst abschliessend aufgeführt.

Es folgt, dass insbesondere keine besonderen Auskünfte und Überwachungen (sog. Spezialfälle) im Pikettdienst erbracht werden. Dies sind Auskünfte beziehungsweise Überwachungen, die keinem Auskunfts- beziehungsweise Überwachungstyp der Verordnung entsprechen (sog. nicht-standardisierte Auskünfte bzw. Überwachungen); vergleiche dazu auch die Ausführungen zu den Artikeln 22 und 25. Im Pikettdienst kann der Dienst ÜPF insbesondere keine Schulungen erbringen und nur eine eingeschränkte Beratung leisten.

Absatz 2 regelt die Leistungen der Mitwirkungspflichtigen ausserhalb der Normalarbeitszeiten. Auf Grund der Verhältnismässigkeit sind die FDA mit reduzierten Überwachungspflichten (Art. 49) sowie die Anbieterinnen abgeleiteter Kommunikationsdienste ohne weitergehende Überwachungspflichten (d. h. diejenigen, die die Voraussetzungen von Art. 50 nicht erfüllen) von diesen Pflichten befreit und somit können Massnahmen, die solche Anbieterinnen betreffen, nicht im Pikett ausgeführt werden. Nicht im Pikett beauftragt und erbracht werden muss, sind des Weiteren die besonderen Auskünfte und Überwachungen nach *Artikel 22*.

4. Abschnitt: Statistiken

Art. 12 Statistik über Überwachungsmassnahmen und Auskünfte

Gemäss geltendem BÜPF führt der Dienst ÜPF eine Statistik über die Überwachungsmassnahmen. Artikel 11 Absatz 1 Buchstabe f des geltenden BÜPF ist dabei die Rechtsgrundlage für die Überwachung des Postverkehrs und Artikel

21 SR **172.220.111.3**

13 Absatz 1 Buchstabe j des geltenden BÜPF diejenige für die Überwachung des Fernmeldeverkehrs.

Artikel 16 Buchstabe k BÜPF wurde am 10. März 2014 durch den Ständerat eingeführt und sieht vor, dass der Dienst ÜPF eine Statistik über die Überwachungen führt.

Weitere Bestimmungen zur Statistik befinden sich in den Artikeln 35 Absatz 3 (Notsuche) und 36 Absatz 2 BÜPF (Fahndung nach verurteilten Personen). Die geltende VÜPF enthält dazu keine Bestimmungen. Auf der Website des Dienstes ÜPF (www.li.admin.ch > Statistik) sind die Statistiken seit 2010 abrufbar. Dabei wird zwischen den Überwachungsmassnahmen, welche im Rahmen eines Strafverfahrens angeordnet werden, und den Notsuchen nach vermissten Personen unterschieden.

Während den Revisionsarbeiten an der VÜPF zeigte sich, dass die heutige Praxis in dieser Verordnung zu verankern ist; dies unter Berücksichtigung von Neuerungen. Grundsätzlich ist es von öffentlichem Interesse, zu wissen, welche Art von Überwachungen und wie viele pro Jahr durchgeführt werden sowie was sie kosten.

Nach *Absatz 1* sind die vom Dienst ÜPF erstellten Statistiken einmal jährlich, in der Regel zu Beginn des Jahres, zu veröffentlichen. Die Veröffentlichung erfolgt im Internet auf der Webseite des Dienstes ÜPF (www.li.admin.ch). Eine Veröffentlichung in anderen Medien (TV, Radio, Zeitungen etc.) ist ebenfalls möglich.

Absatz 2 hält fest, was die Statistiken enthalten müssen. *Buchstabe a bis c* entsprechen der derzeitigen Praxis. Einzig die Fahndung in *Buchstabe c* wird neu aufgeführt. *Buchstabe d bis f* enthalten Neuerungen. In *Buchstabe b* wird das Fürstentum Lichtenstein auch erwähnt, da es als zuständige Behörde im Sinne von Artikel 35 BÜPF betrachtet werden kann, um Notsuchen anzuordnen (siehe Ziff. 3 des Notenaustauschs vom 27. Oktober 2003[22]). In *Absatz 2* wurde auf eine Bestimmung zur Anzahl der nicht genehmigten Überwachungen verzichtet (wie ANITA FETZ und STEFAN ENGLER am 10.03.2014 verlangten; BO 2014 S 112). Zurzeit wären nur die Zwangsmassnahmengerichte in der Lage, solche Statistiken zu liefern, nicht jedoch der Dienst ÜPF, da dieser nur von solchen nicht genehmigten Überwachungsmassnahmen erfährt, die ihm seitens der Staatsanwaltschaft vor dem Entscheid des Zwangsmassnahmengerichts überhaupt zugestellt wurden. Vermutlich gibt es aber eine nicht unwesentliche Anzahl von Überwachungsmassnahmen, die vom Zwangsmassnahmengericht abgelehnt werden, bevor sie beim Dienst ÜPF eintreffen, wovon er naturgemäss keine Kenntnis erhält.

Der Dienst ÜPF ist auch nicht in der Lage, Hinweise auf den Erfolg der Überwachungsmassnahmen zu geben (siehe Anfrage ALINE TREDE 15.5191 "Überwachung des Post und Fernmeldeverkehrs. Wirksamkeit der Vorratsdatenspeicherung" und der Antwort des Bundesrates vom 16.03.2015).

Bei der Redaktion dieses Artikels stellte sich die Frage, ob diejenigen Überwachungen zu zählen sind, welche im vergangenen Jahr angeordnet oder diejenigen, die abgeschlossen wurden. Die heutige Praxis soll nun weitergeführt und alle im vergangenen Jahr angeordneten Überwachungen gezählt werden.

22 SR **0.780.151.41**

Allerdings besteht ein Problem für die Fristberechnung (*Abs. 2 Bst. d*) bei Überwachungen, die in zwei aufeinanderfolgenden Kalenderjahren laufen. Dort ist es nicht möglich, zu Beginn des Jahres bei der Erstellung der Statistiken die Gesamtdauer der im Vorjahr angeordneten Überwachungen zu kennen, wenn diese noch nicht beendet sind. Dieses Problem wird in der Praxis noch zu lösen sein.

Art. 13 Statistik über Überwachungsmassnahmen mit besonderen technischen Geräten und besonderen Informatikprogrammen

In Bezug auf den Einsatz von besonderen technischen Geräten (bspw. IMSI-Catcher) und besonderen Informatikprogrammen (sogenannte "GovWare") stellt Artikel 13 die Ausführungsbestimmung der neuen Artikel 269*bis* Absatz 2 und 269*ter* Absatz 4 der Strafprozessordnung[23] (StPO) für die Staatsanwaltschaften beziehungsweise der neuen Artikel 70*bis* Absatz 2 und 70*ter* Absatz 4 des Militärstrafprozesses vom 23. März 1979[24] (MStP) für die militärischen Untersuchungsrichter dar. Diese neuen Bestimmungen sehen vor, dass der Bundesrat die Einzelheiten regelt. Grundsätzlich sollten sie in den Ausführungsbestimmungen der StPO beziehungsweise in denjenigen der MStP (z. B. in der MStV[25]) zu finden sein. Allerdings kennt das heutige Strafverfahrensrecht keine allgemeine Verordnung im Bereich des Strafverfahrens. Eine neue Verordnung nur zu diesem Zweck zu erstellen, wäre weder angemessen noch verhältnismässig. In Anbetracht, dass die besonderen technischen Geräten und die besonderen Informatikprogramme im weiteren Sinne in Zusammenhang mit der Materie der Überwachung stehen, die im BÜPF und der VÜPF geregelt ist und dass effizienter ist, die Veröffentlichung dieser Statistiken zu zentralisieren, erscheint es sinnvoll, die Kompetenz, diese Statistiken zu publizieren, dem Dienst ÜPF zu überlassen und die Bestimmungen in der VÜPF aufzunehmen; dies erfolgt mit der Schaffung von Artikel 13.

Die Statistiken werden durch die verschiedenen kantonalen Strafverfolgungsbehörden, die Staatsanwälte des Bundes und die verschiedenen militärischen Untersuchungsrichter geführt. Letztere melden diese dem zuständigen Oberauditorat. Deshalb sieht *Absatz 2* vor, dass die von den verschiedenen öffentlichen Behörden erstellten Statistiken dem Dienst ÜPF zu übermitteln sind. Das heisst, die kantonalen Staatsanwaltschaften, die Bundesanwaltschaft und das Oberauditorat haben ihre Statistiken dem Dienst ÜPF zuzustellen. Die Übermittlung muss im ersten Quartal des Folgejahres stattfinden, so dass der Dienst ÜPF alle Statistiken zusammen innert nützlicher Frist publizieren kann.

Im Vorfeld wurden einige Vorbehalte über die Notwendigkeit der Veröffentlichung zum Ausdruck gebracht. Es wurde befürchtet, dass die Veröffentlichung den reibungslosen Ablauf der Ermittlungen gefährden könnte, da die Verwendung von besonderen technischen Einrichtungen zur Überwachung, vor allem aber von GovWare, viel seltener ist als die normalen Überwachungsmassnahmen. Veröffentlichte Statistiken der Kantone, auch wenn diese anonymisiert werden, könnten Rückschlüsse darauf geben, um welches Strafverfahren es sich handelt, dies vor allem in den kleinen Kantonen. Diese Bedenken sind nachvollziehbar. *Absatz 2 Satz 2* sieht deshalb vor, dass die Statistiken den Einsatz von besonderen

23 SR **312.0**
24 SR **322.1**
25 SR **322.2**

technischen Geräten oder besonderen Informatikprogrammen nicht enthalten, wenn deren Einsatz noch nicht abgeschlossen ist. Die kantonalen Strafverfolgungsbehörden oder die Bundesanwaltschaft haben den Dienst ÜPF über das Ende der Überwachungsmassnahme zu orientieren. Damit diese vom Dienst ÜPF in der nächsten Statistik berücksichtigt werden kann. *Absatz 3* hält fest, dass der Dienst ÜPF die Statistik jährlich publiziert. Die Angaben zum Kanton der anordnenden Behörde und die Angaben zur anordnenden Behörde des Bundes werden in der Statistik nicht aufgeführt, um eben die Befürchtungen zu beseitigen, dass mit diesen Informationen Ermittlungen bzw. zukünftige Ermittlungen gefährdet werden könnten.

Etwas schwieriger ist die Frage der Kosten für den Einsatz und die Verwendung von besonderen technischen Geräten oder besonderen Informatikprogrammen. Solche Informatikprogramme werden im Regelfall einmalig gekauft, um dann mit den notwendigen Anpassungen mehrmals in verschiedenen Verfahren verwendet werden zu können. Einzelne Kostenmodelle sehen zudem offenbar Lizenzgebühren für jeden Einsatz vor. Dies erschwert eine korrekte Ausweisung der Kosten. Des Weiteren müssten wohl auch die nur sehr schwer zu ermittelnden Kosten insbesondere für den Personaleinsatz zur Vorbereitung des Aufbringens der GovWare (Polizei, Informatiker, Übersetzer etc.) berücksichtigt werden. Aufgrund dieser Schwierigkeiten wird auf die Angabe der Kosten verzichtet.

2. Kapitel: Postverkehr

Art. 14 Pflichten der PDA

Artikel 14 entspricht im Wesentlichen dem Artikel 14 der VÜPF vom 31. Oktober 2001[26] und regelt die Pflichten der Anbieterinnen von Postdiensten (PDA); siehe auch Artikel 19 BÜPF (Pflichten der Anbieterinnen von Postdiensten), Artikel 20 BÜPF (Informationen vor Anordnung einer Überwachung), die Botschaft zum BÜPF zu dieser Bestimmung[27] und die Erläuterungen hier unten ad Artikel 16.

Art. 15 Anordnung zur Überwachung des Postverkehrs

Artikel 15 entspricht im Wesentlichen dem Artikel 11 der VÜPF vom 31. Oktober 2001[28] und regelt den Inhalt der Überwachungsanordnung im Falle einer Überwachung des Postverkehrs (für den Fernmeldeverkehr, siehe unten die Erläuterungen zu Art. 47).

Für die *Buchstaben j* und *k*, siehe die Erläuterungen zu Artikel 5 (Schutz von Amts- und Berufsgeheimnissen).

26 SR **780.11**
27 BBl **2013** 2729-2731
28 SR **780.11**

Art. 16 Überwachungstypen

Artikel 16 entspricht im Wesentlichen dem Artikel 12 der VÜPF vom 31. Oktober 2001[29] und regelt die verschieden Überwachungstypen im Postverkehr.

Die Lieferumfänge der einzelnen Überwachungstypen sind im Wesentlichen gleich geblieben. Neu ist lediglich, dass im Rahmen der rückwirkenden Überwachung auch der Aufgabeort der Postsendung, soweit verfügbar, anzugeben ist (vgl. Bst. b Ziff. 4). Zu erwähnen ist, dass die Pflicht zur Speicherung und Lieferung von Randdaten - wie nach der bisherigen Regelung - nur im Falle von Postsendungen mit Zustellnachweis besteht. Ein Zustellnachweis im Sinne der Verordnung ist sicherlich gegeben bei Produkten wie eingeschriebenen Postsendungen sowie bei Paketen mit "Track and Trace". Haben die PDA weitere Daten hinterlegt, haben sie auch diese auf Anfrage zu liefern (vgl. Bst. c Ziff. 2).

Angemerkt sei noch, dass die elektronischen Kommunikationsdienste der PDA unter die Fernmeldeüberwachung fallen, beispielsweise E-Mail-Dienste der Post wie PostMail.

3. Kapitel: Fernmeldeverkehr

Aufgrund des raschen technischen Fortschritts und der vielfältigen Implementierungsmöglichkeiten bei den Mitwirkungspflichtigen sind für die zahlreichen Dienste, Optionen und Parameter der Auskunfts- und Überwachungstypen abschliessende Aufzählungen nicht geeignet und es werden stattdessen typische Beispiele aufgeführt.

Der Detaillierungsgrad der Verordnung hat sich im Vergleich zur bisherigen Verordnung stark erhöht und kommt damit dem Wunsch nach mehr Rechtssicherheit entgegen.

1. Abschnitt: Allgemeine Bestimmungen für Auskünfte und Überwachungen

Art. 17 Auskunftsgesuche

Zuerst erscheint es notwendig, zu erklären, wie die Auskunftserteilung (z. B. zum Zwecke der Teilnehmeridentifikation) üblicherweise abläuft: Die Anbieterin sucht in der Regel in den Bestandsdaten, aber auch in den aufbewahrten Randdaten, diejenigen Angaben, auf welche die im Auskunftsgesuch angegebenen Anfragekriterien im angegebenen Zeitraum zutreffen. Sie liefert die entsprechenden Angaben über die Teilnehmenden sowie über die von ihnen in Anspruch genommenen Fernmelde- beziehungsweise abgeleiteten Kommunikationsdienste nach den Vorgaben des Auskunftsgesuchs.

Absatz 1 hält fest, dass die berechtigten Behörden ihre Auskunftsgesuche über das Verarbeitungssystem einzureichen und die betreffenden Mitwirkungspflichtigen grundsätzlich die entsprechenden Daten den betreffenden Behörden ebenfalls über das Verarbeitungssystem zukommen zu lassen haben. Damit sind alle anderen

29 SR **780.11**

Übertragungswege (z. B. elektronisch per E-Mail, postalisch per Brief, telefonisch oder per Fax) nur zulässig, wenn das Verarbeitungssystem beispielsweise aus technischen Gründen nicht zur Verfügung steht oder es sich um eine Ausnahme nach Artikel 18 Absatz 3 oder 4 handelt.

Absatz 2 sieht vor, dass im Auskunftsgesuch die maximale Anzahl der zu liefernden Datensätze anzugeben ist. Das Verarbeitungssystem sorgt dafür, dass die im Auskunftsgesuch wählbare maximale Anzahl der zu liefernden Datensätze die Obergrenzen, die durch das System vorgegeben sind, nicht überschreiten kann. Dies dient zum einen als Schutzmechanismus, um nicht zu viele Ergebnisse zu bekommen, welche Kostenfolgen für die anfragende Behörde nach sich ziehen können. Zum anderen sollen sowohl das Auskunftssystem vor Überlastung geschützt als auch unspezifische Massenabfragen verhindert werden. Die Ergebnisse des Auskunftsgesuchs werden als Datensätze bezeichnet.

Art. 18 Pflichten für die Lieferung von Auskünften

Analog zu Artikel 48 Absatz 1 für die Überwachungspflichten hält *Absatz 1* fest, dass die FDA und die Anbieterin abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten (Art. 21) in der Lage sein müssen, die Auskünfte (Art. 33-46) zu beantworten.

Die Auskünfte gemäss dem 4. und 5. Abschnitt des 3. Kapitels (Art. 33-41) werden grundsätzlich über eine elektronische Schnittstelle des Verarbeitungssystems in einem automatisierten Verfahren beantwortet. Für gewisse Auskunftstypen (Art. 42-46) besteht aber die Möglichkeit, sie manuell zu beantworten (*Abs. 2 in fine*). Dies bedeutet, dass die Antwort nicht automatisiert erteilt werden muss, aber dennoch über das Verarbeitungssystem erfolgt.

Absatz 3 sieht vor, dass die FDA mit reduzierten Überwachungspflichten gemäss Artikel 49 die erwähnten Auskünfte auch schriftlich beantworten können, das heisst ohne die elektronische Schnittstelle des Verarbeitungssystems zu nutzen. Dies ist so vorgesehen, weil viele FDA, die zu dieser Kategorie gehören, nicht über eine solche Schnittstelle verfügen.

In *Absatz 4* wird präzisiert, welche Kategorien von Mitwirkungspflichtigen nicht verpflichtet sind, die Auskünfte gemäss den definierten Auskunftstypen zu erteilen. Sie liefern die ihnen vorliegenden Angaben schriftlich. Es handelt sich um die Anbieterinnen abgeleiteter Kommunikationsdienste ohne weitergehende Auskunftspflichten (diejenigen, die die in Art. 21 festgelegten Voraussetzungen nicht erfüllen) und die Betreiberinnen interner Fernmeldenetze (Art. 1 Abs. 2 Bst. k).

Falls die Anzahl der gefundenen Ergebnisse die im Auskunftsgesuch angegebene maximale Anzahl der zu liefernden Datensätze überschreitet, liefert die Anbieterin nur eine entsprechende Meldung mit der Anzahl der gefundenen Ergebnisse, aber keine Daten (*Abs. 5*). Die anfragende Behörde kann dann das Auskunftsgesuch neu stellen mit verfeinerten Anfragekriterien und/oder mit einem höheren Wert der Höchstzahl der zu liefernden Datensätze, sofern die durch das Auskunftssystem vorgegebene Obergrenze nicht überschritten wird. Falls die anfragende Behörde mehr Ergebnisdatensätze benötigt, als es die Obergrenzen des Verarbeitungssystems zulassen, kann sie das Auskunftsgesuch als besondere Auskunft im Sinne des Artikel 22 Absatz 1 an den Dienst ÜPF stellen.

Art. 19 Erfassung von Angaben zur Person

Artikel 19 entspricht unter anderem dem Artikel 19*a* der VÜPF vom 31. Oktober 2001[30] und bringt die nötigen Präzisierungen an. Er stützt sich dabei namentlich auf die Delegationsnormen an den Bundesrat in Artikel 21 Absatz 1 Buchstabe d, Artikel 22 Absatz 2 und Artikel 23 Absatz 1 BÜPF[31].

Absatz 1 sieht vor, dass bei der Aktivierung von Zugangsmitteln zu Fernmeldediensten oder zu abgeleiteten Kommunikationsdiensten die benutzenden Personen mit geeigneten Mitteln identifiziert werden. Unter "Aktivierung" ist der Zeitpunkt zu verstehen, ab dem ein Teilnehmender den entsprechenden Dienst nutzen kann, z.B. bei bereits aktivierten Zugangsmitteln der Zeitpunkt von dessen Abgabe oder bei einer Embedded SIM, welche fest im Gerät eingebaut ist, die Aktivierung des entsprechenden Profils. Der Begriff *Zugangsmittel* ist die Kurzform von "das für den Zugang zum Fernmeldedienst erforderliche Mittel" (Art. 21 Abs. 1 Bst. e BÜPF). Zu den geeigneten Mitteln der Identifizierung zählt beispielsweise die Angabe einer Mobilfunknummer durch die benutzende Person, an die dann ein Zugangscode per SMS geschickt wird, oder die Identifizierung mittels Kreditkarte.

Absatz 2 sieht vor, dass die benutzenden Personen bei Mobilfunkdiensten anhand eines Reisepasses, einer Identitätskarte oder eines Ausländerausweises im Sinne der Artikel 71 und 71*a* der Verordnung vom 24. Oktober 2007[32] über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE) zu identifizieren sind.

Bei Mobilfunkdiensten ist die Überprüfung der Identität des Kunden anhand eines Ausweises zwingend. Dies entspricht der bisherigen Regelung für vorbezahlte Mobilfunkdienste (Prepaid), welche neu explizit auch auf die Abonnementsverhältnisse ausgedehnt wird. In der Praxis verlangen die Mobilfunkanbieterinnen beim Abschluss von Abonnementen aber bereits seit langem die Vorlage eines Ausweisdokuments. Die Vorgaben für die Überprüfung der Identität der Kunden sind bei Mobilfunkdiensten strenger als bei den anderen Diensten, weil sie besonders weit verbreitet sind und andere Dienste basierend auf diesen Angaben indirekte Identifizierungen vornehmen können sollen.

Die Personendaten sind gemäss dem vorgelegten Ausweis zu erfassen (Art. 23 Abs. 1 BÜPF). Die Anbieterinnen von Fernmeldediensten, die Anbieterinnen von abgeleiteten Kommunikationsdiensten mit weitergehenden Auskunftspflichten gemäss Artikel 21 und die Wiederverkäuferinnen gemäss Artikel 2 Buchstabe f BÜPF müssen dafür sorgen, dass die Erfassung der Angaben zur Person korrekt anhand des vorgelegten Ausweises erfolgt. Zur Kontrolle dient die Ausweiskopie. Angaben, die nicht im Ausweis stehen (z.B. Adresse), sind gemäss den Kundenangaben zu erfassen und entsprechend zu liefern. Die bei der Registrierung erfassten Angaben und die elektronische Ausweiskopie sind von der Wiederverkäuferin an die Anbieterin weiterzuleiten, zu deren Diensten das wiederverkaufte Mittel den Zugang ermöglicht. Wenn der Kunde beziehungsweise die Kundin oder die Anbieterin Angaben ändern (z. B. neue Rechnungsadresse) sind diese ebenfalls zu speichern, es besteht jedoch keine Pflicht zur fortlaufenden Überprüfung und Aktualisierung dieser Daten. Wichtig ist, dass die bei der Registrierung erfassten Daten während der gesamten Dauer der Kundenbeziehung

30 SR **780.11**
31 Siehe Botschaft zum BÜPF vom 27. Februar 2013, BBl **2013** 2734.
32 SR **142.201**

sowie während 6 Monaten nach deren Beendigung durch die Anbieterin aufbewahrt werden müssen (Art. 21 Abs. 2 BÜPF).

Weitere Massnahmen wurden notwendig, weil in der Vergangenheit viele Falschregistrierungen von Teilnehmerdaten stattgefunden haben. Die Ausweiskopie erscheint zurzeit als das geeignetste Mittel, um solchen Falschregistrierungen vorzubeugen. Andere Lösungsansätze wurden bisher keine genannt. Es sind allenfalls weitere Möglichkeiten wie Swiss-ID, elektronische Identität (eID) oder ähnliches denkbar (siehe Bundesgesetz vom 19. Dezember 2003[33] über Zertifizierungsdienste im Bereich der elektronischen Signatur [Bundesgesetz über die elektronische Signatur, **ZertES**] und zukünftiges eID-Gesetz[34]) (siehe Art. 23 Abs. 1 BÜPF).

Der Ausweis muss nicht unbedingt kopiert und in Papierform aufbewahrt werden. Es muss aber eine gut lesbare elektronische Ausweiskopie im System der Anbieterin vorhanden sein (Abs. 2, 2. Satz), egal ob es sich hier um eine Fotografie oder einen Scan handelt (siehe Art. 23 Abs. 1 BÜPF).

Absatz 3 präzisiert die Angaben, die bei natürlichen Personen zu erfassen sind. Die benötigten Angaben (Namen, Vornamen, Geburtsdatum, Art des Ausweises und Ausweisnummer, Adresse) waren schon im Artikel 19*a* der VÜPF vom 31. Oktober 2001[35] vorgesehen und entsprechen der aktuellen Praxis. Falls bekannt ist neu auch der Beruf anzugeben (Art. 21 Abs. 1 Bst. a BÜPF).

Absatz 4 regelt, welche Angaben bei den juristischen Personen zu erfassen sind. Als "verantwortliche natürliche Person" im Sinne von *Buchstabe c* ist eine Person zu verstehen, die gemäss Handelsregistereintrag zeichnungsberechtigt ist. Diese ist nicht unbedingt dieselbe, die die Verantwortung nach dem Obligationenrecht trägt und kann eine andere Person sein als die Person, die den Mobilfunkdienst in Anspruch nimmt (z.B. ein Mitarbeitender). Für letztere genügen, falls vorhanden, die Namen und Vornamen (*Bst. d*).

Absatz 5 verpflichtet die FDA, die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten und die Wiederverkäuferinnen, bei Kundenbeziehungen ohne Abonnementsverhältnis (Prepaid) weitere Angaben zu erfassen. Nicht betroffen sind die einfachen Telefonkarten, die anstelle von Geld zum Telefonieren in den Telefonkabinen verwendet werden können (z. B. die in den Kiosken verkauften, mit Guthaben geladenen "Taxcards")[36]. Gemäss Artikel 1 Buchstabe b der Verordnung vom 9. März 2007[37] über Fernmeldedienste (FDV) ist ein Kunde eine natürliche oder juristische Person, die mit einer Anbieterin von Fernmeldediensten einen Vertrag über die Inanspruchnahme von deren Diensten geschlossen hat. Dies gilt analog auch für Kunden von abgeleiteten Kommunikationsdiensten. Der Grund für die Erfassung dieser weiteren Angaben liegt darin, dass nachvollziehbar sein muss, wer allfällige Falschregistrierungen vorgenommen hat (siehe auch die entsprechende Strafbestimmung in Art. 39 Abs. 1 Bst. c BÜPF).

33 SR **943.03**
34 https://www.egovernment.ch/de/umsetzung/schwerpunktplan/elektronische-identitat/
35 SR **780.11**
36 Siehe Botschaft zum BÜPF vom 27. Februar 2013, BBl **2013** 2709.
37 SR **784.101.1**

Art. 20 Aufbewahrungsfristen

Artikel 20 stellt die Ausführungsbestimmung des Artikels 21 Absatz 2 (Auskünfte über Fernmeldedienste) und des Artikels 22 Absatz 2 BÜPF (Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet) dar.

Absatz 1 sieht vor, dass alle Angaben über die Fernmeldedienste und jene zur Identifikation der Täterschaft bei Straftaten über das Internet grundsätzlich während der Dauer der Kundenbeziehung sowie während 6 Monate nach deren Beendigung aufzubewahren und elektronisch zu liefern sind. Zu den *Angaben über die Fernmeldedienste* gehören auch die Angaben zur Person gemäss Artikel 19 Absätze 1-3.

In Ausführung von Artikel 21 Absatz 2 zweiter Satz und Artikel 22 Absatz 2 zweiter Satz BÜPF bestimmt *Absatz 2* die Angaben, die nur während 6 Monaten aufzubewahren und zu liefern sind, damit kein Widerspruch zur Aufbewahrungsfrist nach Artikel 26 Absatz 5 BÜPF besteht. Diese Aufbewahrungsfrist ist eine kürzere Frist als die von Absatz 1. Diese sind die Liste der Geräteidentifikatoren, zum Beispiel IMEI, MAC-Adresse (siehe Art. 34 Abs. 1 Bst. d und 39 Abs. 1 Bst. d), sowie die Angaben nach Artikel 35 Absatz 1, Artikel 36 Absatz 1 und Artikel 37 Absatz 1.

Siehe auch die Übergangsbestimmungen in Artikel 45 Absatz 3 BÜPF.

Art. 21 Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten

Abgeleitete Kommunikationsdienste werden immer mehr eingesetzt und nehmen entsprechend immer mehr an Bedeutung zu. Die gewöhnlichen Anbieterinnen abgeleiteter Kommunikationsdienste haben im Bereich der Fernmeldeüberwachung aufgrund der gesetzlichen Vorgaben weniger weitreichende Pflichten. Sie haben eine Überwachung lediglich zu dulden und die ihnen vorliegenden Angaben herauszugeben, die für die Durchführung der Fernmeldeüberwachung notwendig sind. Wenn eine Straftat über das Internet begangen wird, kann es jedoch vorkommen, dass diese Minimalpflicht nicht ausreicht. Aus diesem Grund hat der Gesetzgeber in Artikel 22 Absatz 4 BÜPF dem Bundesrat die Kompetenz eingeräumt, auch den Anbieterinnen abgeleiteter Kommunikationsdienste weitergehende Auskunftspflichten aufzuerlegen. Bei den zu erfüllenden Pflichten handelt es sich um dieselben Pflichten, die von den FDA zu erfüllen sind. Die Anbieterinnen abgeleiteter Kommunikationsdienste, die weitergehende Pflichten haben, müssen somit allen Pflichten nach Artikel 22 Absatz 1 und 2 BÜPF nachkommen.

Absatz 1 konkretisiert die einzelnen Voraussetzungen, welche erfüllt werden müssen, damit eine Anbieterin abgeleiteter Kommunikationsdienste weitergehende Auskunftspflichten hat. Eine Anbieterin hat dann weitergehende Auskunftspflichten, wenn sie 50 Auskunftsaufträge in den letzten 12 Monaten auszuführen hatte (wobei der 30. Juni als Stichtag dient) oder einen Jahresumsatz von 100 Millionen Franken in zwei aufeinander folgenden Geschäftsjahren erzielt. Das zweite Kriterium wird dadurch weiter eingeschränkt, dass nur solche Anbieterinnen in die Pflicht gezogen werden, bei denen ein grosser Teil ihrer Geschäftstätigkeit im Anbieten von abgeleiteten Kommunikationsdiensten besteht und ihre Dienste zudem von mindestens 5000 benutzenden Personen in Anspruch

genommen werden. Weil die Schwellenwerte zum Schutz der Schweizer KMU sehr hoch angesetzt sind, werden zahlenmässig relativ wenigen Anbieterinnen abgeleiteter Kommunikationsdienste weitergehende Auskunftspflichten auferlegt.

Absatz 2 bildet den sogenannten Konzerntatbestand. Kontrolliert eine Anbieterin eine oder mehrere rechnungspflichtige Unternehmen, werden sie bei der Berechnung der Grössen nach Absatz 1 Buchstabe a und b als eine Einheit betrachtet. Es wird dabei auf die Regelung von Artikel 963 Absatz 1 und 2 Obligationenrecht (OR) verwiesen, welche sinngemäss Anwendung findet. Zu erwähnen ist, dass die Muttergesellschaft und das kontrollierte Unternehmen nur in Bezug auf die von ihnen angebotenen Kommunikationsdienste als eine Einheit behandelt werden.

Absatz 3 sieht für die Anbieterinnen eine Meldepflicht vor für den Fall, dass die Anbieterin realisiert, dass sie die Schwellenwerte nach Absatz 1 Buchstabe a oder b unter- oder überschreitet. Dafür stellt der Dienst ÜPF geeignete Meldemechanismen zur Verfügung.

Absatz 4 sieht vor, dass eine Anbieterin, welche die Voraussetzungen nach Absatz 1 erfüllt, innert zwei Monaten die für die Auskunftserteilung erforderlichen Daten speichern und innert zwölf Monaten auskunftsbereit sein muss. Die Frist beginnt ab Kenntnisnahme der Bedingung von Absatz 1 zu laufen, das heisst, sobald die Anbieterin feststellt, dass sie die Voraussetzungen nach Absatz 1 Buchstabe a oder b erfüllt. Der Dienst ÜPF unterstützt die Anbieterin beratend bei der Erfüllung ihrer Pflichten.

Art. 22 Besondere Auskünfte und Überwachungen

Alle gängigen Auskunfts- und Überwachungstypen sind in den Artikeln 23 und 24 erwähnt und in den 4.–6. (Art. 33-46) beziehungsweise 8.–11. Abschnitten (Art. 52–68) des 3. Kapitels geregelt.

Die nicht explizit in dieser Verordnung aufgeführten Auskünfte und Überwachungen sowie vorläufig die Überwachungen nach Artikel 58 und 59 stellen sogenannte Spezialmassnahmen dar. Diese werden vom Dienst ÜPF oder durch von diesem beauftragte Personen durchgeführt. Dies entspricht der heutigen Praxis nach den Artikeln 17 Absatz 5 und 25 Absatz 5 VÜPF vom 31. Oktober 2001[38]. Diese Bestimmungen wurden mit der Änderung vom 23. November 2011 (in Kraft seit dem 1. Januar 2012) eingefügt, um die Befugnis des Dienstes ÜPF, die Durchführung von Überwachungsmassnahmen, die nicht explizit in der VÜPF aufgeführt sind, die aber durch die Strafverfolgungsbehörden angeordnet und von den Zwangsmassnahmengerichten genehmigt wurden, gegenüber den betroffenen Anbieterinnen verfügen zu können, gesondert zu regeln. Gemäss dem Entscheid des Bundesverwaltungsgerichts vom 23. Juni 2011 (A-8267/2010) müssen die betroffenen Anbieterinnen die Durchführung solcher Überwachungsmassnahmen dulden. Sie müssen dem Dienst ÜPF die Schnittstellen zur Verfügung stellen, die bereits vorhanden sind. Dasselbe gilt, wenn Dritte von der Anbieterin als Erfüllungsgehilfen zur Durchführung von Auskünften und Überwachungen beigezogen worden sind (*Abs. 2*).

38 SR **780.11**

Zu den Duldungspflichten der Anbieterin zählt auch der Zugang zu den Anlagen (Art. 51), insbesondere die kostenlose Zurverfügungstellung bestehender Netzzugänge zu öffentlichen Fernmeldenetzten.

Art. 23 Auskunftstypen

Artikel 23 dient als Kurzübersicht über die verschiedenen Auskunftstypen, welche in den Abschnitten 4 bis 6 des 3. Kapitels (Art. 33-46) näher geregelt sind. Unter einem Auskunftstyp versteht man eine in dieser Verordnung näher bestimmte Art und Weise des Gesuchs und der Erteilung von Auskünften über die Daten nach den Artikeln 21 und 22 BÜPF im Zusammenhang mit Fernmeldediensten oder abgeleiteten Kommunikationsdiensten.

Die Auskunftstypen gemäss den Artikeln 33 bis 40 zeichnen sich durch eine hohe Regelungsdichte aus, was für deren automatisierte Bearbeitung notwendig ist. Die Auskunftstypen gemäss den Artikeln 33 bis 40 entsprechen im Wesentlichen den bisherigen einfachen Auskünften A0. Die automatisierte Bearbeitung solcher Auskunftsgesuche ist angesichts ihrer sehr grossen Anzahl unabdingbar (zum Vergleich: 181'835 Abfragen in 2015[39]).

Die Automatisierung erfordert genaue Vorgaben, insbesondere hinsichtlich der einzelnen Parameter und Datentypen. Diese Vorgaben sind vom Departement in der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) festgelegt (Art. 31 Abs. 3 BÜPF).

Neben den stark formalisierten Auskunftstypen gibt es weitere Auskünfte (Art. 40-46), die auch mittels manueller Verfahren erteilt werden können.

Allen Auskünften gemeinsam ist die Tatsache, dass die gemäss Artikel 15 BÜPF berechtigten Behörden die Abfragen an den Dienst ÜPF stellen, der sie dann an die entsprechenden Mitwirkungspflichtigen vermittelt. Die Mitwirkungspflichtigen erteilen die gewünschten Auskünfte wiederum an den Dienst ÜPF, der die Ergebnisse an die anfragende Behörde weiterleitet. Soweit wie technisch möglich, erfolgt die Vermittlung der Auskunftsgesuche und Ergebnisse automatisiert über das Auskunftssystem des Dienstes ÜPF.

Neu sind die Auskunftstypen gemäss ETSI-Norm TS 102 657 organisiert. Die Auskunftstypen sind nach Dienstkategorien unterteilt. Diese Unterteilung ist durch die ETSI-Norm vorgegeben. Da die Produkte der Anbieterinnen mehrere Dienstkategorien umfassen können (zum Beispiel Mobilfunkabonnement mit den Dienstkategorien Netzzugang sowie Telefonie- und Multimediadienste) sollte in der Praxis je ein Auskunftsgesuch pro Auskunftstyp eingeholt werden, um alle Dienste abzufragen.

Für die am häufigsten unter den Auskunftsgesuchen vertretenen Dienstkategorien *Netzzugangsdienste* sowie *Telefonie- und Multimediadienste* gibt es eine Unterteilung in die Typen "Auskünfte über Teilnehmende" (Art. 33 und 38) und die Typen "Auskünfte über Dienste" (Art. 34 und 39). Diese Aufteilung entspricht in etwa den bisherigen Auskünften A0 und A1 und dient dazu, den Umfang der Informationen pro Auskunftstyp zu begrenzen, um die automatisierte Bearbeitung zu erleichtern und zu beschleunigen.

[39] Statistik des Dienstes ÜPF: www.li.admin.ch/de/themen/statistik

Bei den weniger häufig angefragten Dienstkategorien *E-Mail-Dienste* sowie *andere Fernmelde- oder abgeleitete Kommunikationsdienste* wurde auf diese Unterteilung verzichtet.

Bei der Dienstkategorie *Netzzugangsdienste* kommen noch drei spezifische Auskunftstypen (Art. 35-37) für die Zwecke der Identifikation der Benutzerschaft bei Straftaten über das Internet (Art. 22 BÜPF) hinzu.

Art. 24 Überwachungstypen

Artikel 24 dient als Kurzübersicht über die verschiedenen Überwachungstypen, die in den Abschnitten 8 bis 11 des 3. Kapitels (Art. 52–68) näher geregelt sind. Unter einem Überwachungstyp versteht man eine in dieser Verordnung näher bestimmte Art und Weise der Überwachung eines oder mehrerer Fernmeldedienste beziehungsweise abgeleiteter Kommunikationsdienste (Art. 31 Abs. 1 BÜPF). Unterschieden wird zwischen Echtzeitüberwachungen (Abs. 1), rückwirkenden Überwachungen (Abs. 2) sowie Notsuchen (Abs. 3) und Fahndungen (Abs. 4).

Die Überwachungstypen der Echtzeitüberwachung sind so aufgebaut, dass die Strafverfolgungsbehörden bei den wichtigsten Dienstkategorien neu die Möglichkeit haben, entweder nur die Lieferung in Echtzeit der Randdaten oder die Lieferung in Echtzeit der Inhalts- und Randdaten zu verlangen (Abs. 1). Dadurch soll eine Möglichkeit geschaffen werden, die Schwere des Grundrechtseingriffs abstufen zu können.

Inhaltsdaten (z. B. Gespräche, E-Mail-Texte und Anhänge) können nur im Rahmen einer Echtzeitüberwachung beschafft werden. Bei rückwirkenden Überwachungen (Randdaten der rückwirkenden Überwachung, auch Randdaten des vergangenen Fernmeldeverkehrs oder Vorratsdaten genannt) werden hingegen Inhaltsdaten weder gespeichert noch herausgegeben (zum Begriff Randdaten siehe auch die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels).

Die Überwachung des Fernmeldeverkehrs ist so aufgebaut, dass für die wichtigsten Dienstkategorien eigenständige Überwachungstypen definiert sind. Dadurch wird einerseits dem Bestimmtheitsgebot Rechnung getragen und anderseits den Vorgaben der internationalen Standards entsprochen. Die Dienstkategorien werden unterteilt in Netzzugangsdienste und Anwendungen (engl.: application). Zu den Anwendungen gehören dabei die Telefonie- und Multimediadienste, die E-Mail-Dienste sowie andere Fernmelde- und abgeleitete Kommunikationsdienste.

Traditionell waren bei der Telefonie Netzzugang und Anwendung identisch (Telefonanschluss). Somit genügte es in der Regel, den Anschluss zu überwachen. Im Zuge des technischen Fortschritts gibt es jedoch immer mehr Kommunikationsdienste, bei denen der Netzzugang fast beliebig sein kann. Eine Überwachung am Netzzugang (Anschluss) wäre bei solchen Diensten wenig erfolgversprechend. Dies umso mehr, wenn die Kommunikation zudem noch von der Anbieterin oder den Endgeräten beziehungsweise Clients verschlüsselt wird. Dies wird am Beispiel der nomadischen Internettelefonie (VoIP) deutlich: Die Zugangsdaten des Teilnehmenden können beispielsweise in einer App auf dem Smartphone gespeichert sein. Der Teilnehmende kann das Smartphone an einem beliebigen Internetzugang verwenden (z. B. im Hotel, im Büro, am Flughafen) und kann mit Hilfe der App die Internet-Telefoniedienste in Anspruch nehmen. Da die Strafverfolgungsbehörden zum einen nicht von vornherein wissen, welche Internetzugänge der überwachte Teilnehmende benutzen wird und zum anderen

sehr viele Internetzugänge (z. B. WLAN-Zugangspunkte) in Frage kommen können, ist es effizienter, die Überwachung bei der Anbieterin der Anwendung, (im Beispiel bei der Anbieterin des Internettelefoniedienstes) vorzunehmen. Dadurch werden alle Kommunikationen erfasst, die über den überwachten Internettelefoniedienst geführt werden, unabhängig davon, welchen Netzzugang die überwachte Person benutzt. Die Anbieterin hat zudem eine allfällige von ihr angebrachte Verschlüsselung zu entfernen. So werden die überwachten Kommunikationsinhalte für die Strafverfolgungsbehörden auch auswertbar.

Da die Produkte der Anbieterinnen mehrere Dienstkategorien umfassen können (z. B. Mobilfunkabonnement mit der Dienstkategorie Netzzugang und der Dienstkategorie Telefonie- und Multimediadienste), kann es für eine vollständige Überwachung erforderlich sein, dass mehrere Überwachungstypen für den gleichen Zielidentifikator angeordnet werden müssen. Zu beachten ist des Weiteren, dass Fernmeldeprodukte mehrere unterschiedliche Dienstangebote enthalten können, welche zu verschiedenen Überwachungstypen gehören. Wenn beispielsweise ein Smartphone komplett in Echtzeit überwacht werden soll (Inhalt und Randdaten), muss die Behörde zwei Überwachungen anordnen: (die erste vom Typ RT_16_NA_CC_IRI für den mobilen Internetzugang und die zweite vom Typ RT_18_TEL_CC_IRI für den Mobiltelefoniedienst). Diese Trennung hat eine administrative und eine technische Ursache. In administrativer Hinsicht soll es den anordnenden Behörden wie bisher ermöglicht werden, die Überwachungen der einzelnen Fernmeldedienste entsprechend den Bedürfnissen der Untersuchung unabhängig voneinander anordnen zu können. Technisch gesehen unterscheidet sich die Überwachung des mobilen Internetzugangs grundsätzlich von der Überwachung der Anwendung Mobiltelefonie. Durch die Trennung in zwei verschiedene Überwachungstypen wird den unterschiedlichen Abläufen bei der Aktivierung und Durchführung der Überwachungen auf Seiten der Mitwirkungspflichtigen Rechnung getragen.

Art. 25 Verzicht auf die Standardisierung

Unter Standardisierung eines Auskunfts- oder Überwachungstyps durch das EJPD versteht man die Regelung von dessen technischen und administrativen Einzelheiten in der Departementsverordnung VD-ÜPF (zum Begriff Auskunftstyp siehe die Erläuterungen zu Art. 23; zum Begriff Überwachungstyp siehe die Erläuterungen zu Art. 24). Die Voraussetzungen für diese Standardisierung sind zum einen die Existenz der entsprechenden internationalen Standards und zum anderen die Machbarkeit und Verhältnismässigkeit ihrer Umsetzung in der Praxis.

Sollten diese Voraussetzungen für bestimmte Typen bei Inkraftsetzung dieser Verordnung noch nicht gegeben sein, verzichtet das EJPD vorerst auf deren Standardisierung.

Gemäss Artikel 31 Absatz 3 BÜPF soll das EJPD selber bestimmen können, welches die «gängigen», d.h. für eine Standardisierung geeigneten Typen sind. Die vom Bundesrat definierten und die vom EJPD standardisierten Typen sollen nicht streng aneinander gebunden sein, damit dem EJPD in eigener Verantwortung der Spielraum für eine Erweiterung, Reduktion oder Verschiebung des Kreises der standardisierten Typen bleibt und es dafür nicht immer gleichzeitig eine Revision der Bundesratsverordnung VÜPF erwirken muss.

2. Abschnitt: Qualitätssicherung

Art. 26 Direktschaltungen aus technischen Gründen

Artikel 26 regelt den Fall, dass es dem Dienst ÜPF aufgrund technischer Umstände nicht möglich ist, die Daten aus Überwachungsmassnahmen zu empfangen und im Verarbeitungssystem zu speichern. In solchen Fällen soll die Möglichkeit eingeräumt werden, dass die betroffene Mitwirkungspflichtige die Überwachungsdaten ohne Umweg über den Dienst ÜPF direkt an die betreffende Behörde übermittelt (Direktschaltung im Sinne von Art. 17 Bst. c und Art. 26 Abs. 1 Einleitungssatz BÜPF). Die Daten werden somit nicht im vom Dienst ÜPF betriebenen Verarbeitungssystem aufgezeichnet, sondern die betreffende Behörde hat die Daten selbst aufzuzeichnen.

Stellt der Dienst ÜPF fest, dass eine Direktschaltung aus technischen Gründen notwendig ist, informiert er die beteiligten Mitwirkungspflichtigen, die anordnende sowie die von dieser bezeichnete Behörde. Eine Direktschaltung bedingt einerseits, dass die Mitwirkungspflichtigen in der Lage sein müssen, die Überwachungsdaten direkt an die Strafverfolgungsbehörden weiterzuleiten. Andererseits müssen auch die Strafverfolgungsbehörden in der Lage sein, solche Daten von den Mitwirkungspflichtigen zu empfangen.

Die Regelung sagt allerdings nichts darüber aus, wie lange die Anbieterinnen und die Strafverfolgungsbehörden Zeit haben, um sich im Ernstfall bereit zu machen, eine solche Direktschaltung umzusetzen. Realistischerweise ist aber von einem Zeitbedarf von mehreren Monaten auszugehen. Der Dienst ÜPF steht den betroffenen Mitwirkungspflichtigen sowie den betroffenen Strafverfolgungs-behörden zudem beratend zur Seite.

Ähnlich wie bei einer Überwachungsmassnahme, die über das Verarbeitungssystem des Dienstes ÜPF abgewickelt wird, ist der Überwachungsauftrag beim Dienst ÜPF einzureichen. Der Dienst ÜPF sendet den Auftrag an die betreffende Mitwirkungspflichtige und macht sie darauf aufmerksam, dass der in Frage stehende Auftrag aufgrund technischer Gründe nicht über das Verarbeitungssystem des Dienstes ÜPF, sondern direkt an die bezeichnete Behörde auszuleiten ist. Gleichzeitig wird das Vorgehen auch der betreffenden Behörde zur Kenntnis gebracht. Die Mitwirkungspflichtige bestätigt dem Dienst ÜPF den Eingang des Auftrages und ob sie in der Lage ist, die Direktschaltung selbständig auszuführen. Auch die betreffende Behörde hat den Dienst ÜPF darüber zu informieren, ob sie in der Lage ist, die Überwachungsdaten direkt zu empfangen. Wenn sowohl die Mitwirkungspflichtige als auch die betreffende Strafverfolgungsbehörde die Machbarkeit der Direktschaltung bestätigt haben, führt die Mitwirkungspflichtige die Überwachung entweder selber aus oder lässt sie durch einen Dritten ausführen und bestätigt dem Dienst ÜPF, dass der Auftrag ausgeführt wurde; vgl. zur Ausführung eines Überwachungsauftrages Artikel 11 der VD-ÜPF sowie die dazugehörigen Ausführungen im Erläuterungsbericht der erwähnten Verordnung.

Für die Ausleitung der Daten aus einer Direktschaltung kommen die gleichen Schnittstellenspezifikationen zur Anwendung wie für die Ausleitung zum

Verarbeitungssystem. Ähnlich wie bei einer Überwachungsmassnahme, die über das Verarbeitungssystem des Dienstes ÜPF läuft, kann auch eine Direktschaltung so lange aktiv bleiben, wie es von der anordnenden Behörde bestimmt ist. Verlängerungen sind ebenfalls möglich. Eine bestehende Direktschaltung kann nicht auf das Verarbeitungssystem des Dienstes ÜPF migriert werden, sondern die entsprechende Überwachung ist bei Bedarf von der Behörde neu anzuordnen und vom Dienst ÜPF an die Mitwirkungspflichtige zu beauftragen. Die Neuanordnung unterliegt des Weiteren den üblichen Gebühren und Entschädigungen.

Die Direktschaltung unterliegt den Beschränkungen gemäss Art. 271 StPO und Art. 70b MStP (siehe Art. 271, Abs. 2 StPO und Art. 70b, Abs. 2 MStP) (siehe Botschaft zum BÜPF vom 27. Februar 2013, BBl **2013** 2780).

Art. 27 Qualität der übermittelten Daten

Damit ein reibungsloser Ablauf der Überwachung nicht beeinträchtigt wird, muss unter anderem auch die Qualität der übermittelten Daten gewahrt sein. Diese Bestimmung definiert deshalb die Anforderungen an die Qualität der übermittelten Daten beziehungsweise unter welchen Voraussetzungen eine solche als gewahrt gilt.

Nach *Absatz 1* ist die Qualität der Daten gewahrt, wenn die Datenausleitung den vom Departement festgelegten Anforderungen entspricht (*Bst. a*), diese ohne Datenverlust und ohne Unterbrüche erfolgt (*Bst. b*) und die übermittelten Überwachungsdaten mit dem im Überwachungsauftrag bezeichneten Fernmeldeverkehr beziehungsweise die übermittelten Auskunftsdaten mit dem im Auskunftsgesuch bezeichneten Daten übereinstimmen (*Bst. c*). Dabei muss nur die Ausleitung der Überwachungs- beziehungsweise Auskunftsdaten ohne Datenverlust und ohne Unterbrüche erfolgen. Sind die der Mitwirkungspflichtigen vorliegenden Daten bereits unvollständig, ist die erforderliche Qualität gewahrt, wenn diese ohne Datenverlust und ohne Unterbrüche ausgeleitet werden. Ausgeleitet werden kann also nur, was im Netz der Mitwirkungspflichtigen vorliegt. Die Qualität der Überwachungsdaten kann daher nicht besser sein als die der vorschriftsmässig überwachten Dienste. Ebenso kann die Qualität der Auskunftsdaten nicht besser sein als die der vorschriftsmässig erfassten und gespeicherten Bestands- und Randdaten.

Absatz 2 und *Absatz 3* regeln die Verantwortlichkeiten bei der Sicherstellung der Qualität. Für die Qualität der übermittelten Auskunfts- und Überwachungsdaten ist somit die Mitwirkungspflichtige verantwortlich. Der Dienst ÜPF steht der betreffenden Mitwirkungspflichtigen dabei beratend zur Seite. Eine Mitwirkungspflichtige ist auch dann für die Qualität der übermittelten Daten verantwortlich, wenn sie Dritte mit der Ausführung der Überwachung beauftragt hat.

Stellt der Dienst ÜPF oder die betreffende Mitwirkungspflichtige fest, dass die Qualität der übermittelten Daten mangelhaft ist, haben sie sich unverzüglich gegenseitig zu informieren (*Abs. 4*). Falls insbesondere Leistungen betroffen sind, die während des Pikettdienstes erbracht werden (siehe Art. 11) hat diese Meldung sofort telefonisch an die entsprechenden Kontaktstellen zu erfolgen. Denkbar ist auch, dass Qualitätsmängel durch die Strafverfolgungsbehörden festgestellt werden. In diesem Fall hat die betreffende Strafverfolgungsbehörde den

festgestellten Mangel an den Dienst ÜPF zu melden und dieser informiert anschliessend die betreffende Mitwirkungspflichtige.

Sowohl der Dienst ÜPF als auch die Mitwirkungspflichtigen mit Überwachungspflichten betreiben ein Monitoring zur Qualitätskontrolle. Die Details sind in der VD-ÜPF geregelt.

Bei Störungen analysieren die betreffende Mitwirkungspflichtige und der Dienst ÜPF diese unverzüglich und informieren die Gegenpartei umfassend und schnellstmöglich über die Analyseergebnisse. Liegt die Störung auf Seiten der Mitwirkungspflichtigen, hat sie dem Dienst ÜPF eine formelle Störungsmeldung in schriftlicher Form unter Angabe des genauen Ausfallzeitraums, der Problembeschreibung, einer chronologischen Übersicht der eingeleiteten Massnahmen und des Problemstatus zukommen zu lassen. Die Störungsmeldung hat dabei spätestens am nächsten Arbeitstag zu erfolgen. Die Mitwirkungspflichtige hat zudem dem Dienst ÜPF so rasch wie möglich mitzuteilen, wie lange die Störung nach ihrer Einschätzung dauern sollte. Zur umfassenden Information gehört auch die Übermittlung der einzelnen Abklärungsergebnisse und der dazugehörigen Daten an die Gegenseite. Diese Daten dienen zur Untermauerung der Analyseergebnisse und werden gegebenenfalls von der Gegenseite für ihre Analyse benötigt. Der Dienst ÜPF hört die betreffende Mitwirkungspflichtige an und legt gemeinsam mit dieser den jeweiligen Schweregrad (zum Beispiel: kritisch, schwerwiegend, geringfügig) der Störung fest. Die betreffende Mitwirkungspflichtige behebt die festgestellten Mängel innerhalb der durch das Departement für die einzelnen Schweregrade festgelegten Reparaturzeiten und informiert den Dienst ÜPF schriftlich und regelmässig in den durch das Departement festgelegten Zeitabständen über die weiteren eingeleiteten Massnahmen und den neusten Problemstatus. Nach der Störungsbehebung hat die Anbieterin dem Dienst ÜPF unverzüglich eine schriftliche Abschlussmeldung zu senden, welche die Angaben der Störungsmeldung vervollständigt und gegebenenfalls präzisiert.

Die Randdaten der Echtzeitüberwachung sind gemäss den technischen Möglichkeiten der Schnittstellenspezifikation zu speichern und unverzüglich nachzuliefern. Sollten die Randdaten der Echtzeitüberwachung nicht mehr verfügbar oder unvollständig sein, hat die Mitwirkungspflichtige auf Anweisung des Dienstes ÜPF die entsprechenden Randdaten der rückwirkenden Überwachung unverzüglich zu liefern (siehe Art. 4 Abs. 3).

Art. 28 Testschaltungen

Nach *Absatz 1* werden Testschaltungen ausgeführt, um die Qualität der Datenausleitung der Mitwirkungspflichtigen an den Dienst ÜPF und die Strafverfolgungsbehörden sicherzustellen (*Bst. a*), die Auskunfts- und Überwachungsbereitschaft der Mitwirkungspflichtigen zu überprüfen (*Bst. b*), die Systeme des Dienstes ÜPF zu testen (*Bst. c*), zu Schulungszwecken (*Bst. d*) sowie um Referenzdaten zu erzeugen (*Bst. e*).

Unter einer *Testschaltung* versteht man die technische Überwachung eines Fernmeldedienstes (z.B. Mobilabonnement, Prepaid-SIM-Karte, Festnetzanschluss) beziehungsweise abgeleiteten Kommunikationsdienstes (z.B. Messaging-Dienst, Webmail) zu den in *Absatz 1* aufgeführten Zwecken. Die dabei verwendeten Geräte und Software werden als *Testausstattung* bezeichnet. Dies

können beispielsweise Endgeräte wie Smartphones sein oder auch Simulatoren in Form von Software, welche die testende Organisation ausschliesslich zu diesem Zweck einsetzt. Bei einer Testschaltung wird das Ziel der Überwachung als *Testtarget* bezeichnet. Die im Rahmen einer Testschaltung verwendeten beziehungsweise erzeugten Daten (z.B. Telefongespräche, SMS, Internetverkehr) werden als *Testdaten* bezeichnet. Die *Testdaten* werden unter Kenntnisnahme aller Beteiligten lediglich mit dem Ziel verwendet oder erzeugt, um die unter Absatz 1 aufgeführten Zwecke zu erfüllen. Damit wird sichergestellt, dass alle an einer Testüberwachung beteiligten Kommunikationspartner und deren Fernmeldeverkehr nur fiktiv sind. Testtargets, Testdienste und Testausstattungen stehen nur denjenigen Personen des Dienstes ÜPF, der Mitwirkungspflichtigen und der Strafverfolgungsbehörden zur Verfügung, die zur Benutzung von Testschaltungen berechtigt sind.

Da die Testdaten lediglich für Testschaltungen benutzt werden, fallen solche Daten nicht unter das Fernmeldegeheimnis. Testschaltungen bedürfen somit auch keiner Genehmigung durch die zuständige richterliche Instanz und auch die Voraussetzungen von Artikel 269 Absatz 1 StPO müssen nicht erfüllt sein. Da es bei Testschaltungen des Dienstes ÜPF keine mit dem Verfahren befasste Behörde gib, kann der Dienst ÜPF vom Inhalt der Testdaten seiner Testschaltungen Kenntnis nehmen, ohne eine vorgängige Zustimmung einholen zu müssen (Art. 18 Abs. 2 BÜPF).

Für Testschaltungen führt der Dienst ÜPF gesonderte Überwachungsakten im Sinne von Artikel 9. Bei Testschaltungen erfasst der Dienst ÜPF lediglich die Angaben zur verantwortlichen Person, deren Organisationseinheit (Name und Adresse), den Verwendungszweck des Testtargets und die Namen der berechtigten Personen, welche die Daten der Testschaltung bearbeiten dürfen. Hingegen werden auch Testschaltungen ähnlich wie normale Überwachungen protokolliert. Der Dienst ÜPF protokolliert also auch bei Testschaltungen die Datenbearbeitung aller Testtargets.

Die Strafverfolgungsbehörden können gemäss *Absatz 4* ebenfalls Testschaltungen auf eigene Kosten durchführen, um die Qualität des ausgeleiteten Fernmeldeverkehrs sicherzustellen oder für Schulungszwecke. Hierzu müssen sie beim Dienst ÜPF eine entsprechende Anordnung einreichen und die entsprechenden Gebühren entrichten. Damit eine Strafverfolgungsbehörde Testschaltungen beantragen kann, wird vorausgesetzt, dass sie eine Person und deren Stellvertretung benennt, welche für die Verwaltung von Testtargets, Testdiensten und Testausstattungen der betreffenden Organisationseinheit verantwortlich sind und das Recht haben, beim Dienst ÜPF die erforderlichen Anordnungen für Testschaltungen einzureichen. Auf eigene Kosten bedeutet, dass die betreffenden Strafverfolgungsbehörden auch die Entschädigungen zu tragen haben, welche an die Mitwirkungspflichtigen für die Durchführung der von den Strafverfolgungsbehörden erwünschten Testschaltungen ausgerichtet werden. Das heisst die Strafverfolgungsbehörden müssen auch für die Durchführung von Testschaltungen dem Dienst ÜPF die entsprechenden Gebühren gemäss Gebührenverordnung zahlen, inklusive der an die beteiligten Mitwirkungspflichtigen zu entrichtenden Entschädigungen. Die anfallenden Gebühren und Entschädigungen sind in der GebV-ÜPF geregelt. Die aus ihren Testschaltungen gewonnenen Daten können die Strafverfolgungsbehörden dabei entweder auf das vom Dienst ÜPF betriebene Verarbeitungssystem ausleiten lassen

oder eine direkte Ausleitung (siehe Erläuterungen zur Direktschaltung in Art. 26) an sich selber veranlassen. Für die Testschaltungen der Strafverfolgungsbehörden gilt Artikel 18 Absatz 2 BÜPF sinngemäss.

Beim Überwachungsauftrag hat der Dienst ÜPF den Vermerk anzubringen, dass es sich im konkreten Fall um eine Testschaltung handelt. Ist der Dienst ÜPF bei der Erzeugung von Testdaten auf die Hilfe der Mitwirkungspflichtigen angewiesen, kann er sie entsprechend damit beauftragen (*Abs. 2*). Des Weiteren muss die Mitwirkungspflichtige dem Dienst ÜPF die für dessen Testschaltungen erforderlichen eigenen Fernmeldedienste beziehungsweise abgeleiteten Kommunikationsdienste kostenlos und dauerhaft zur Verfügung stellen (*Abs. 4*). Das bedeutet, dass namentlich die Grundgebühren, die Aktivierungsgebühren, die wiederkehrenden Gebühren sowie alle Arten von Kommunikations- und Nutzungsgebühren dieser Dienste durch die Mitwirkungspflichtige zu finanzieren sind. So zum Beispiel: Die Mitwirkungspflichtige stellt dem Dienst ÜPF die erforderliche Anzahl von SIM-Karten kostenlos zur Verfügung, aktiviert kostenlos die erforderlichen Dienste und berechnet für deren Nutzung keinerlei Gebühren.

Die nicht-proprietären, das heisst marktüblichen Endgeräte werden dagegen vom Dienst ÜPF beschafft und finanziert. Falls die Fernmeldedienste beziehungsweise die abgeleiteten Kommunikationsdienste einer Mitwirkungspflichtigen jedoch proprietäre Endgeräte erfordern, hat sie diese für die Testschaltungen des Dienstes ÜPF erforderlichen Endgeräte ebenfalls kostenlos dem Dienst ÜPF zur Verfügung zu stellen.

Testschaltungen, die auf Ersuchen der Strafverfolgungsbehörden durchgeführt werden, müssen ähnlich den gewöhnlichen Überwachungen einen formellen Weg durchlaufen. Die betreffende Strafverfolgungsbehörde muss zuerst beim Dienst ÜPF einen entsprechenden Antrag einreichen. Sie muss auch angeben, wie lange die Testschaltungen aktiv bleiben sollen, wobei die Maximaldauer 12 Monate beträgt. Der Dienst ÜPF prüft, ob der Antrag seinen Vorgaben entspricht und, ob dieser von einer dazu berechtigten Person eingereicht wurde. Sind die erwähnten Voraussetzungen erfüllt, übermittelt der Dienst ÜPF die entsprechenden Überwachungsaufträge zur Aktivierung der Testschaltungen an die betreffenden Mitwirkungspflichtigen. Auch in diesem Fall hat der Dienst ÜPF den Vermerk anzubringen, dass es sich im konkreten Fall um eine Testschaltung handelt. Die berechtigten Personen der Strafverfolgungsbehörde können auf Antrag ihre Testschaltungen jeweils für maximal weitere 12 Monate gebührenpflichtig verlängern lassen. Der Dienst ÜPF sendet spätestens 3 Monate vor Ablauf einer Testschaltung eine entsprechende Erinnerungsmeldung an die berechtigten Personen der Strafverfolgungsbehörde. Sind die erwähnten Voraussetzungen für die Verlängerung erfüllt, bleibt die betreffende Testschaltung aktiv. Andernfalls beendet der Dienst ÜPF die betreffende Testschaltung, indem er den entsprechenden Überwachungsauftrag zur termingerechten Aufhebung der Testschaltung an die betreffende Mitwirkungspflichtige übermittelt.

3. Abschnitt: Sicherstellung der Auskunfts- und Überwachungsbereitschaft

Art. 29 Überprüfung der Auskunfts- und Überwachungsbereitschaft

Jede FDA und jede Anbieterin abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten gemäss Artikel 21 muss in der Lage sein (Auskunftsbereitschaft), die Auskünfte gemäss Artikel 33–46, die durch sie angebotene Dienste betreffen, zu erteilen oder durch Dritte erteilen zu lassen (vgl. Art. 18).

Jede FDA und jede Anbieterin abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 50 muss in der Lage sein (Überwachungsbereitschaft), die Überwachungen gemäss Artikel 52–68, die durch sie angebotene Dienste betreffen, auszuführen oder durch Dritte ausführen zu lassen (vgl. Art. 48). Davon ausgenommen sind die FDA mit reduzierten Überwachungspflichten gemäss Artikel 49.

Um die Auskunfts- beziehungsweise Überwachungsbereitschaft zu belegen, müssen die erwähnten Anbieterinnen neu nachweisen können, dass sie die Erteilung der Auskünfte beziehungsweise die Ausführung der Überwachungen nach dem anwendbaren Recht sicherstellen können (*Abs. 1*).

Gemäss *Absatz 2* ist der Nachweis erbracht, wenn die gemäss den Vorgaben des Dienstes ÜPF durchzuführenden Tests erfolgreich abgeschlossen worden sind (*Bst. a*) und die Anbieterin in einem vom Dienst ÜPF erarbeiteten Fragebogen bestätigt, dass sie die Vorgaben bezüglich der standardisierten Auskünfte beziehungsweise Überwachungen erfüllt, die nicht mittels Tests nachgewiesen werden. Da die Anbieterinnen die Möglichkeit haben, die ihnen zukommenden Auskunfts- und Überwachungspflichten durch einen Dritten zu erfüllen, können sie vorsehen, dass auch der Nachweis der Auskunfts- und Überwachungsbereitschaft durch diesen Dritten erbracht wird. Bei der Überprüfung der Auskunfts- und Überwachungsbereitschaft wird in diesem Fall auch die Drittperson aufgefordert, den erforderlichen Nachweis zu erbringen. Möglich ist, dass der Nachweis in Zusammenarbeit mit der betreffenden Anbieterin erbracht wird. Die Verantwortung für den Nachweis liegt in jedem Fall bei der betreffenden Anbieterin.

Bei der Überprüfung der Auskunfts- und Überwachungsbereitschaft nimmt der Dienst ÜPF gemäss *Absatz 3* folgende Aufgaben wahr: Er legt nach Rücksprache mit der betreffenden Anbieterin einen verbindlichen Zeitplan für die Durchführung der Tests fest und definiert die von der Anbieterin auszuführenden Testfälle. Er kontrolliert die sich aus den Tests ergebenden Resultate (*Bst. a*), wertet den Fragebogen aus (*Bst. b*), protokolliert die Prüfungsvorgänge (*Bst. c*) und wenn die betreffende Anbieterin auskunfts- und überwachungsbereit ist, stellt er der Anbieterin eine Bestätigung aus (*Bst. d*). Die erwähnten Protokolle sind vom Dienst ÜPF während der Gültigkeitsdauer der Bestätigung und bis zwei Jahre nach deren Ablauf aufzubewahren (*Bst. e*). Die Protokolle können einerseits im Falle eines Rechtsstreits als Beweismittel herangezogen werden, andererseits können sie bei der nächsten Überprüfung der Auskunfts- und Überwachungsbereitschaft als Hilfsmittel dienen.

Die Bestätigung hält dabei fest, dass die Anbieterin für bestimmte Gültigkeitskriterien in der Lage ist, die Datenausleitung gemäss den Vorgaben des Departements auszuführen und sie somit die Auskunfts- und Überwachungsbereitschaft sicherstellt (*Abs. 4*).

Art. 30 Gültigkeitsdauer der Bestätigung

Ergibt die Überprüfung der Auskunfts- und Überwachungsbereitschaft, dass die betreffende Mitwirkungspflichtige bereit beziehungsweise in der Lage ist, entsprechende Aufträge vorschriftsgemäss auszuführen, wird der betreffenden Mitwirkungspflichtigen eine Bestätigung ausgestellt (vgl. hierzu die Erläuterungen zu Art. 29).

Gemäss *Absatz 1* ist diese Bestätigung während 3 Jahren gültig. Massgebend für die Fristberechnung ist dabei das Ausstelldatum der Bestätigung durch den Dienst ÜPF.

Absatz 2 sieht vor, dass der Dienst ÜPF nach Ablauf der Gültigkeitsdauer die Bestätigung jeweils um weitere drei Jahre verlängern kann, wenn die Mitwirkungspflichtige bescheinigt, dass seit der Erteilung der Bestätigung keine Umstellungen vorgenommen wurden, welche die Datenausleitung, die Auskunfts- oder die Überwachungsbereitschaft beeinflussen. Hierfür muss die Mitwirkungspflichtige beim Dienst ÜPF einen entsprechenden Antrag stellen und die unter Absatz 2 aufgeführten Bescheinigungen beilegen.

Absatz 3 auferlegt der Mitwirkungspflichtigen eine Meldepflicht. Die Mitwirkungspflichtige hat demnach die Pflicht, den Dienst ÜPF unverzüglich darüber in Kenntnis zu setzen, falls sie feststellt, dass sie nicht mehr auskunfts- oder überwachungsbereit ist.

Art. 31 Abnahmeverfahren

Diese Bestimmung gibt dem Departement die Kompetenz, den Ablauf des Verfahrens für die Abnahme der technischen Systeme sowie das Verfahren zur Überprüfung der Auskunfts- und Überwachungsbereitschaft zu regeln (siehe auch Art. 31 Abs. 3 BÜPF).

Art. 32 Ungültigerklärung der Bestätigung der Auskunfts- und Überwachungsbereitschaft

Ist eine FDA oder eine Anbieterin abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten nicht mehr in der Lage, die Auskünfte beziehungsweise die Überwachungen, die durch sie angebotene Dienste betreffen, zu erteilen beziehungsweise auszuführen, erklärt der Dienst ÜPF die bereits durch ihn erteilte Bestätigung der Auskunfts- und Überwachungsbereitschaft unverzüglich für ungültig. Es ist möglich, dass die Anbieterin nur in Bezug auf bestimmte von ihr angebotene Dienste nicht mehr auskunfts- und/oder überwachungsbereit ist. In diesem Fall bezieht sich die Ungültigkeitserklärung lediglich auf den betreffenden Dienst und den nicht mehr sichergestellten Auskunfts- und/oder Überwachungstyp. Die Ungültigkeitserklärung bezieht sich nicht auf die anderen von der Anbieterin angebotenen Dienste. In einem solchen Fall ist, in Bezug auf jene Dienste, bei denen die Auskunfts- und Überwachungsbereitschaft gewährleistet ist, eine separate Bestätigung zu erstellen.

Bei Bedarf kann auch in diesem Fall eine erneute Überprüfung angeordnet werden, bevor eine allfällige Bestätigung ausgestellt wird. Aus dieser Bestätigung muss klar hervorgehen, auf welche Dienste sich die Bestätigung bezieht. Ist in Bezug auf einen angebotenen Dienst die Auskunftsbereitschaft zwar gegeben, jedoch nicht die Überwachungsbereitschaft, ist dies ebenfalls in der Bestätigung beziehungsweise in der Ungültigkeitserklärung entsprechend festzuhalten.

Eine Ungültigkeitserklärung wird dann in Erwägung gezogen, wenn die Anbieterin selbst einen entsprechenden Antrag stellt (*Bst. a*), wenn Erkenntnisse vorliegen, nach welchen die Anbieterin in einem oder mehreren Fällen nicht in der Lage ist, die Datenausleitung, die Auskunfts- oder die Überwachungsbereitschaft sicherzustellen (*Bst. b*) oder wenn bestätigte Aussagen der Anbieterin nicht der Wahrheit entsprechen (*Bst. c*).

4. Abschnitt: Auskunftstypen für Netzzugangsdienste

Art. 33 Auskunftstyp IR_1_NA: Auskünfte über Teilnehmende von Netzzugangsdiensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von Netzzugangsdiensten. Dieser Auskunftstyp entspricht im Wesentlichen den bisherigen Auskünften A0 und teilweise A1 (*Abs. 2 Bst. j und k*). Möglich sind neu Abfragen nach der Unternehmens-Identifikationsnummer (*Abs. 2 Bst. g*), dem Teilnehmeridentifikator (*Abs. 2 Bst. h*) und dem Dienstidentifikator (*Abs. 2* Bst. l).

Unter Netzzugangsdiensten sind Fernmeldedienste zu verstehen, die unmittelbar (z.B. DSL-Internetanschluss) oder mittelbar (z.B. Virtual Private Network, VPN) den Zugang zu öffentlichen Fernmeldenetzen wie dem Internet ermöglichen. Beim VPN ist Folgendes zu beachten: Zwischen dem unmittelbaren Internetzugang des VPN-Kunden und der VPN-Anbieterin besteht ein VPN-Tunnel. Die VPN-Kunden treten im Internet mit einer IP-Adresse der VPN-Anbieterin auf und nicht mit der von ihrer unmittelbaren Internet-Zugangsanbieterin zugeteilten IP-Adresse, das heisst die Zugriffe der VPN-Kunden ins Internet haben als Quelladresse eine IP-Adresse der VPN-Anbieterin. Die IP-Adresse des unmittelbaren Internetzugangs der VPN-Kunden ist nur für die VPN-Anbieterin sichtbar. Daher müssen die VPN-Anbieterinnen ebenfalls Auskünfte über ihre Teilnehmenden und Dienste geben können.

Dieser Auskunftstyp ist nach dem ETSI-Standard TS 102 657 aufgebaut. Er kombiniert die allgemeinen Teilnehmendeninformationen (generic subscriber info) mit den wichtigsten Angaben zu den Netzzugangsdiensten des Teilnehmenden. Weitere spezifische Angaben über Netzzugangsdienste können über den Auskunftstyp IR_2_NA (Art. 34) abgefragt werden.

Der Artikel kann mit einem Beispiel veranschaulicht werden: Die Person X bezieht die folgenden Dienste bei der Anbieterin Y: drei Mobilabonnemente (mit Telefonie und Internet), zehn Prepaid-Karten (nur Telefonie) und zwei Internetzugangsdienste im Festnetz. Die Strafverfolgungsbehörde, die den Namen und die Adresse der Person X kennt, möchte wissen, welche Dienste die Person X

bei der Anbieterin Y bezieht. Zu diesem Zweck stellt sie die Auskunftsgesuche IR_1_NA (Art. 33) und IR_6_TEL (Art. 38). Anbieterin Y antwortet zum Auskunftstyp IR_1_NA (Art. 33) mit fünf Ergebnissen (zählt als fünf Datensätze, siehe die Erläuterungen zu Art. 17 Abs. 2) und zum Auskunftstyp IR_6_TEL (Art. 38) mit 13 Ergebnissen (zählt ebenfalls als 13 Datensätze).

In *Absatz 1* werden die in der Antwort zu liefernden Angaben über Teilnehmende von Netzzugangsdiensten aufgeführt; siehe Artikel 21 Absatz 1 BÜPF (Auskünfte über Fernmeldedienste) und Artikel 22 Absatz 2 und 4 BÜPF (Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet).

Gemäss *Buchstabe a* ist ein im Bereich der Anbieterin eindeutiger Identifikator (z. B. Kundennummer) mitzuteilen, falls die Anbieterin dem Teilnehmenden einen solchen zugeteilt hat.

Die in *Buchstabe b* aufgeführten Angaben zur Person werden im Einzelnen bei Artikel 19 erläutert.

Nachfolgend werden die einzelnen Ziffern des *Buchstabens c* erläutert:

- Bei dem in *Ziffer 1* genannten "eindeutigen Identifikator, welcher die Anbieterin bezeichnet", handelt es sich um eine administrative Nummer, die der Dienst ÜPF der Anbieterin zuteilt, um sie eindeutig zu identifizieren.

- Der "eindeutige Dienstidentifikator" gemäss *Ziffer 2* bezeichnet den in Anspruch genommenen Fernmelde- oder abgeleiteten Kommunikationsdienst des Teilnehmenden. Diese Bezeichnung muss mindestens im Bereich der Anbieterin eindeutig sein (z. B. Telefonnummer, Benutzername, Bezeichnung des Breitbandanschlusses, E-Mail-Adresse).

- Unter dem Begriff *Beginn* des "Zeitraums des Dienstbezugs" gemäss *Ziffer 3* ist der Zeitpunkt (Datum und Uhrzeit) der Aufnahme der Kundenbeziehung zu verstehen. Die eigentliche Aktivierung des Dienstes kann unter Umständen später erfolgt sein. So ist es möglich, dass z. B. eine Prepaid-SIM-Karte an einem Tag verkauft und die dazugehörigen Personendaten am selben Tag erfasst wurden, die SIM-Karte jedoch erst einige Tage später aktiviert wurde. Aktivierung bedeutet in diesem Sinne, dass der Dienst ab diesem Zeitpunkt für den Teilnehmenden nutzbar ist. Falls zutreffend ist der Zeitpunkt der Aktivierung mitzuteilen. Das *Ende-Datum* bezeichnet den Zeitpunkt, ab dem der Dienst für den Teilnehmenden dauerhaft nicht mehr nutzbar ist. Eine vorübergehende Sperrung des Dienstes gilt hingegen nicht als Ende des Dienstbezugs. Der Zusatz "gegebenenfalls" bedeutet, dass nur dann ein *Ende-Datum* zu liefern ist, wenn der Dienst für den Teilnehmenden dauerhaft nicht mehr nutzbar ist.

- Gemäss *Ziffer 4* können optional Angaben über zusätzliche Optionen oder Einschränkungen des Netzzugangsdienstes in für Menschen lesbarer Form übermittelt werden, z.B. "mit statischer IP-Adresse", "Datenvolumen max. 1 GB" (siehe ETSI-Standard TS 102 657, Tabelle E.2).

- Die Standortangaben des Festnetzzugangs gemäss *Ziffer 5* bestehen aus der Installationsadresse des Netzzugangs, wie sie die Anbieterin für den Teilnehmenden vermerkt hat.

- Bei den Zuständen des Dienstes gemäss *Ziffer 6* kann die Anbieterin ihre üblichen Bezeichnungen übermitteln, da eine Umwandlung in standardisierte Bezeichnungen zu viel Aufwand verursachen würde. Mit Gültigkeitszeitraum

ist die Zeitspanne (Beginn-Datum und gegebenenfalls End-Datum) gemeint, wann die Zustandsangabe gültig ist beziehungsweise war.

- Gemäss *Ziffer 7*, falls zutreffend, alle im Zusammenhang mit diesem Dienst zugeteilten statischen IP-Adressen, IP-Präfixe, IP-Adressbereiche und Netzmasken beziehungsweise Präfixlängen und jeweils deren Gültigkeitszeitraum.

- Gemäss *Ziffer 8* sind im Falle von vorbezahlten Fernmeldediensten zusätzlich nach Artikel 21 Absatz 1 Buchstabe e BÜPF und Artikel 19 Absatz 1 die Abgabestelle und der Name der Person, die das für den Zugang zum Fernmeldedienst erforderliche Mittel abgegeben hat, mitzuteilen.

- Gemäss *Ziffer 9* sind, falls zutreffend, alle im Zusammenhang mit dem angefragten Netzzugangsdienst durch die Anbieterin in den Bestandsdaten registrierten Nummern der SIM-Karten (ICCID) und deren Aktivierungs- und gegebenenfalls Deaktivierungsdatum zu liefern.

- Gemäss *Ziffer 10* ist im Falle von Mobilfunkdiensten die IMSI (International Mobile Subscriber Identity) zu liefern. Diese global eindeutige Nummer dient zur Identifikation des Mobilfunk-Teilnehmenden gegenüber dem Netz.

- Gemäss *Ziffer 11* ist der Typ des Dienstes zu liefern. Diese Angabe dient zur Mitteilung, ob es sich um einen vorbezahlten Dienst (prepaid) oder ein Abonnement handelt (postpaid).

- Gemäss *Ziffer 12* ist, falls zutreffend, der alternative Teilnehmeridentifikator für den Netzzugangsdienst zu liefern. Diese Angabe ist nur dann erforderlich, falls es neben dem eindeutigen Teilnehmeridentifikator gemäss Buchstabe a noch einen weiteren Teilnehmeridentifikator für diesen Netzzugangsdienst gibt.

In *Absatz 2* sind die Anfragekriterien aufgeführt. Mit diesen erfolgt die Anfrage durch die Strafverfolgungsbehörde an die Anbieterin über das Auskunftssystem des Dienstes ÜPF. Dabei muss mindestens ein Anfragekriterium im Auskunftsgesuch angegeben werden. Bei Verwendung eines Anfragekriteriums gemäss den Buchstaben a bis d ist noch ein weiteres Anfragekriterium (*Bst. a–k*) anzugeben, damit die Anfrage spezifisch genug ist. Die Anfragekriterien gemäss den *Buchstaben e-k* sind hingegen eindeutig, so dass die Angabe **eines** solchen Anfragekriteriums bereits ausreicht.

In *Buchstabe a* sind Name(n) und Vorname(n) zu einem Anfragekriterium zusammengefasst. Dies ermöglicht eine freie Kombination bei der Anfrage. Einerseits kann es vorkommen, dass bei der Registrierung Vornamen und Nachnamen bei der Erfassung vertauscht werden; anderseits ist es nicht immer klar, welches der Vorname beziehungsweise der Nachname ist (z.B. Thomas Peter), oder eine Person hat mehrere Vornamen beziehungsweise Nachnamen (z.B. Heydi Núñez Gómez).

Hausnummern sind nicht immer vorhanden, daher der Zusatz *allenfalls* in *Buchstabe d*.

In *Buchstabe i* sind IP-Adressen als Anfragekriterium ausgeschlossen, da für die Abfrage von IP-Adressen die spezifischen Auskunftstypen IR_3_IP (Art. 35),

IR_4_IP(NAT) (Art. 36) und IR_5_NAT (Art. 37) zur Verfügung stehen (siehe die Erläuterungen zu Art. 35, 36 und 37).

Art. 34 Auskunftstyp IR_2_NA: Auskünfte über Netzzugangsdienste

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Netzzugangsdienste, der auf dem ETSI-Standard TS 102 657 basiert. Damit werden weitere Angaben gemäss Artikel 21 Absatz 1 Buchstabe d BÜPF eingeholt.

In *Absatz 1* sind die in der Antwort zu liefernden Angaben und in *Absatz 2* die Anfragekriterien aufgeführt.

Bei Absatz 1 *Buchstabe d* ist zu beachten, dass die Liste der im Anfragezeitraum **tatsächlich benutzten** Geräteidentifikatoren zu liefern ist. Diese Informationen hat die Anbieterin aus den gespeicherten Randdaten zu gewinnen, ohne jedoch die Randdaten selbst herauszugeben (zum Begriff Randdaten siehe auch die einleitenden Erläuterungen zum 10. Abschnitt des 3. Kapitels). Das heisst, aus der Antwort darf nicht ersichtlich sein, wann, wie und wo die Benutzung im Einzelnen stattgefunden hat.

Art. 35 Auskunftstyp IR_3_IP: Identifikation der Benutzerschaft bei eindeutig zugeteilten IP-Adressen

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte zur Identifikation der Benutzerschaft bei eindeutig zugeteilten IP-Adressen, der sich am ETSI-Standard TS 102 657 orientiert. Damit werden die Angaben gemäss Artikel 22 Absatz 2 BÜPF eingeholt. Dieser Auskunftstyp entspricht den bisherigen Auskünften A0.1 (statische IP-Adresse) und A0.2 (dynamische IP-Adresse). In diesem Auskunftstyp werden alle Anfragen nach IP-Adressen vereinheitlicht, da man es einer IP-Adresse nicht ansieht, ob sie eindeutig zugeteilt ist beziehungsweise war. Falls die IP-Adresse nicht eindeutig zugeteilt war, teilt die Anbieterin dies in der Antwort mit und die anfragende Behörde kann dann ein neues Auskunftsgesuch des Typs IR_4_IP (NAT) (Art. 36) stellen, das allerdings weitere Anfragekriterien benötigt (siehe Erläuterungen zu Art. 36).

Unter dem Begriff *eindeutig zugeteilte IP-Adresse* ist zu verstehen, dass zu einem beliebigen Zeitpunkt maximal ein Teilnehmender oder eine Teilnehmende mit dieser Adresse im Internet aufgetreten ist. Dies trifft zum einen auf die statischen IP-Adressen und zum anderen auf die eindeutig zugeteilten dynamischen IP-Adressen zu. Da man wie erwähnt einer IP-Adresse nicht ansieht, ob sie eindeutig zugeteilt war oder ist, verschafft erst das Ergebnis dieses Auskunftstyps Klarheit. Wichtig ist die Angabe eines präzisen, sekundengenauen Zeitpunkts im Auskunftsgesuch, da bei eindeutig zugeteilten dynamischen IP-Adressen der Zuteilungszeitraum sehr kurz sein kann und damit falschpositive Ergebnisse erzielt werden könnten. Insbesondere bei ausländischen Zeitangaben ist auf die korrekte Zeitzone zu achten.

Die Anbieterin führt die Suche für den angefragten Zeitpunkt plus/minus ein Toleranzintervall von einigen Sekunden durch. Dieses Toleranzintervall ist wegen der möglichen Ungenauigkeiten der Systemuhren erforderlich und wird in der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) definiert, wo auch die einzelnen Schritte zur Beantwortung eines solchen Auskunftsgesuchs konkretisiert werden.

Art. 36 Auskunftstyp IR_4_IP (NAT): Identifikation der Täterschaft bei nicht eindeutig zugeteilten IP-Adressen (NAT)

Dieser Auskunftstyp ist neu und behandelt ein spezifisches Problem der Teilnehmeridentifikation im Falle von nicht-eindeutig zugeteilten IP-Adressen. Er basiert auf dem ETSI-Standard TS 102 657. Bei der sogenannten Network Address Translation (NAT) können sich viele Tausend Benutzer und Benutzerinnen gemeinsam die gleiche öffentliche IP-Adresse teilen. Eine Teilnehmeridentifikation ist bei NAT daher nur mit erhöhtem technischem Aufwand möglich.

Carrier-grade NAT (cgNAT) bedeutet Network Address Translation (NAT) auf Ebene der Anbieterin (Carrier). Dabei werden den Teilnehmenden im Netz der Zugangsanbieterin private IP-Adressen zugeteilt, die nur innerhalb des Netzes der Zugangsanbieterin gültig sind. Diese werden bei Zugriffen ins Internet an den Netzgrenzen der Zugangsanbieterin zum Internet in eine gemeinsame öffentliche Quell-IP-Adresse übersetzt (viele Teilnehmende teilen sich gleichzeitig eine öffentliche IP-Adresse). Die Unterscheidung der vielen einzelnen Internetverbindungen erfolgt mittels Port-Nummern. Diese Adressübersetzung muss für jedes eingehende und ausgehende IP-Paket durchgeführt werden. Bei nicht-deterministischen Verfahren führt das Gerät (Router) Zuordnungstabellen und speichert für jede Internetverbindung (Kontext) den Zeitstempel, die Quelle und das Ziel (jeweils IP-Adresse und Portnummer), die zugehörige private IP-Adresse und Portnummer des Teilnehmenden sowie die Art des Transportprotokolls. Bei deterministischen NAT-Verfahren werden Adressen und Portnummern mit einem Algorithmus übersetzt und können später wieder zurückgerechnet werden und somit entfällt die Notwendigkeit der Speicherung der Ziel-IP-Adressen und -Portnummern durch die Zugangsanbieterin für die Zwecke der Teilnehmeridentifikation.

Für den mobilen Internetzugang (z.B. GPRS, UMTS, LTE) werden schon seit längerem NAT-Verfahren eingesetzt. Die Hauptgründe dafür sind die Knappheit von öffentlichen IPv4-Adressen und Sicherheitsüberlegungen wie das sogenannte Topology Hiding, das heisst damit man von aussen nicht auf die Struktur des Netzes schliessen kann. Da mittlerweile kaum noch öffentliche IPv4-Adressen verfügbar sind, sind die Zugangsanbieterinnen dazu übergegangen, cgNAT mehr und mehr auch für fixe Internetzugänge einzusetzen.

Im Gegensatz zu IPv4 stehen bei IPv6 genügend Adressen zur Verfügung und es ist damit zu rechnen, dass cgNAT langfristig an Bedeutung verlieren wird. Im Moment ist aber eher eine zunehmende Bedeutung aufgrund der erschöpften Reserven von IPv4-Adressen und des stark wachsenden mobilen Datenverkehrs (z.B. Smartphones, Tablets) zu beobachten.

Absatz 1 Buchstabe a bestimmt, welche Angaben in der Antwort zu liefern sind, falls die Identifikation erfolgreich war. Gemäss *Buchstabe b* ist in der Antwort der Grund (z.B. kein Treffer, mehrere Treffer) mitzuteilen, falls die Identifikation nicht erfolgreich war.

Absatz 2 bestimmt, welche Angaben das Auskunftsgesuch enthalten muss:

- die öffentliche Quell-IP-Adresse (*Bst. a*), das heisst die gemeinsam benutzte öffentliche IP-Adresse, die im Internet als Originating IP sichtbar ist.

- falls für die Identifikation notwendig, d.h. im Falle eines NAT-Verfahrens, die öffentliche Quell-Port-Nummer (*Bst. b*), die im Internet als Originating Port sichtbar ist.

  Hinweis: Die private Quell-IP-Adresse und -Portnummer (private IP/port) sind nur der Zugangsanbieterin bekannt.
- falls für die Identifikation notwendig, d.h. im Falle eines nicht-deterministischen NAT-Verfahrens, die öffentliche Ziel-IP-Adresse (z.B. Webserver), die Ziel-Portnummer und der Typ des Transportprotokolls, z.B. TCP, UDP (*Bst. c, d und e*);
- der Zeitpunkt nach Datum und Uhrzeit (*Bst. f*). Hinweis: Die Zeitangabe muss exakt und der Suchbereich möglichst eng sein, damit falsch-positive Treffer vermieden werden (siehe Erläuterungen zu Art. 35)..

Zusammengefasst sind für das Vorgehen folgende Schritte vorgesehen:

- 1. Schritt (gehört zu den Vorarbeiten und ist nicht Teil dieses Auskunftstyps): IP-History für das gesuchte Benutzerkonto bei der Betreiberin des Internet-Dienstes (Server-Seite) beschaffen.

- 2. Schritt: Auskunftsgesuch an die Internetzugangsanbieterin (Angabe der Verbindungsdetails eines konkreten Login-Ereignisses gemäss IP-History).

Details zum 1. Schritt: Abfrage der sogenannte IP-History für ein bestimmtes Benutzerkonto bei der Dienstanbieterin auf der Server-Seite, d.h. am "Ziel" (Beispiel: Blog-Betreiber, Webmail oder soziales Netzwerk)

Als Resultat erhält die Strafverfolgungsbehörde ein Verbindungsprotokoll mit allen Angaben zur Bestimmung der Internetzugänge, von wo aus die Zugriffe auf das gesuchte Benutzerkonto erfolgten: Quelle der Verbindung (IP-Adresse + Port), Zielserver (IP-Adresse + Port), Zeitstempel, Typ des Protokolls. Mit Hilfe dieser Angaben kann dann im 2. Schritt die Identifikation der Benutzerschaft erfolgen.

Details zum 2. Schritt: Beispielsweise könnte eine Suche für einen mobilen Internetzugang wie folgt ablaufen. Anhand der 3 bis 6 Angaben des Auskunftsgesuchs sucht die Zugangsanbieterin in den bei ihr gespeicherten NAT-Übersetzungsdaten die private IP Adresse und Portnummer (die dem gesuchten Teilnehmenden zum gesuchten Zeitpunkt zugeordnet waren, d.h. Source IP (private IP/port). Danach wird, anhand der im 1. Schritt gefundenen privaten IP-Adresse und Portnummer sowie dem Zeitstempel, die MSISDN oder IMSI des Teilnehmenden gesucht. Zum Schluss werden anhand der im 2. Schritt gefundenen MSISDN oder IMSI die entsprechenden Personendaten des Teilnehmenden gesucht.

Es sind auch ähnliche Abfragen möglich, zum Beispiel bei Dual-Stack Lite (DS Lite).

Seit der Version V1.14.1 des ETSI-Standards TS 102 657, welche im März 2014 veröffentlicht wurde, gibt es eine standardisierte Datenstruktur für NAT-Daten (Annex E.3 "ASN.1 definitions for network access services").

Die technischen Herausforderungen bei der Speicherung und Abfrage von NAT-Übersetzungsdaten bestehen darin, dass die Anbieterinnen erhebliche Datenmengen speichern und die Effizienz der Suchvorgänge sicherstellen müssen. Die vielen unterschiedlichen IP-Verbindungen, die gleichzeitig über den NAT-Router laufen, werden anhand der oben beschriebenen Parameter unterschieden.

Ein einzelner Benutzer benutzt dabei in der Regel Dutzende bis Hunderte von IP-Verbindungen gleichzeitig. Die Quell-Portnummern und die übersetzten Portnummern werden zyklisch wieder frei gegeben und neu zugeteilt. Beispielsweise wird bei Smartphones die Internet-Verbindung bei Nichtgebrauch abgebaut, um Batteriestrom zu sparen. Daher bekommt das Smartphone beim Neuaufbau der Internetverbindung eine neue (private) IP-Adresse zugeteilt. Daraus ergibt sich ein enorm dynamischer Ablauf, der erhebliche Datenmengen generiert. Aktuell geht man in grossen Schweizer Mobilnetzen von etwa einer Milliarde NAT-Übersetzungsvorgängen pro Tag aus.

Die Strafverfolgungsbehörden müssen sich bewusst sein, dass es bei diesem Auskunftstyp möglich ist, dass es zu keinem Ergebnis beziehungsweise zu mehrdeutigen Ergebnissen kommen kann, insbesondere wenn nicht alle erforderlichen Parameter in der Anfrage angegeben wurden. Die Treffergenauigkeit kann beispielsweise durch die Korrelation mehrerer Anfragen erhöht werden. Die Speicherung der NAT-Übersetzungsdaten durch die Anbieterinnen löst nicht allein das Problem der Teilnehmeridentifikation im Internet. Häufig speichern die Zielserver keine Quell-Portnummern und keine exakten Zeitstempel. Aufgrund des hochdynamischen Ablaufs des NAT werden aber möglichst vollständige und präzise Angaben benötigt, um falschpositive Ergebnisse zu vermeiden.

Zum Schluss ein Hinweis: Je nach NAT-Verfahren müssen die Ziel-IP-Adressen und -Portnummern aller Teilnehmenden, falls diese Daten Randdaten im Sinn des BÜPF und der VÜPF sind, durch die Zugangsanbieterin nur während 6 Monaten gespeichert werden (Art. 21 Abs. 2 2. Satz und 22 Abs. 2 2. Satz und Abs. 4 BÜPF sowie Art. 20 Abs. 2).

Art. 37 Auskunftstyp IR_5_NAT: Auskünfte über NAT-Übersetzungsvorgänge

Dieser Auskunftstyp ist neu und dient der Identifikation der Benutzerschaft bei Straftaten über das Internet gemäss Artikel 22 BÜPF. Er basiert auf dem ETSI-Standard TS 102 657.

Hinweis: Der NAT-Übersetzungsvorgang wird im Folgenden als *NAT-Operation* bezeichnet. Es gibt zwei Abfragemöglichkeiten ("vor" und "nach" der NAT-Operation sind zeitlich und aus Sicht der angefragten Mitwirkungspflichtigen zu verstehen):

- Abfragemöglichkeit 1

  Es sind die Angaben **nach** der NAT-Operation bekannt, gesucht sind die Angaben **vor** der NAT-Operation, z.B. bekannt ist die öffentliche Quell-IP-Adresse und Portnummer nach der NAT-Operation), gesucht ist die IP-Adresse vor der NAT-Operation.
  Analog zum Artikel 35 Absatz 2 muss das Auskunftsgesuch über NAT-Operationen folgende Angaben enthalten (*Abs. 2*):

  - Die Quell-IP-Adresse und Port-Nummer nach der NAT-Operation (*Bst. a und b*), z.B. die gemeinsam benutzte öffentliche IP-Adresse sowie die Portnummer, die im Internet als sog. "Source IP/port" sichtbar sind;
  - den Typ des Transportprotokolls, z.B. TCP (*Bst. e*);
  - den Zeitpunkt der NAT-Operation nach Datum und Uhrzeit (*Bst. f*).

- Falls für die Identifikation notwendig (hängt vom NAT-Verfahren ab), muss das Auskunftsgesuch die öffentliche Ziel-IP-Adresse und Ziel-Portnummer (*Bst. c und d*) des Zielservers enthalten.

- Abfragemöglichkeit 2

  Es sind die Angaben **vor** der NAT-Operation bekannt, gesucht sind die Angaben **nach** der NAT-Operation - bekannt ist die IP-Adresse **vor** der NAT-Operation (z.B. private IP-Adresse), gesucht ist die IP-Adresse **nach** der NAT-Operation (z.B. öffentliche Quell-IP-Adresse)
  Analog zum Artikel 36 Absatz 2 muss das Auskunftsgesuch über NAT-Operationen folgende Angaben enthalten (*Abs. 2*):

  - Die Quell-IP-Adresse und Port-Nummer vor der NAT-Operation (*Bst. a und b*), z.B. die private IP-Adresse der Internetzugangsanbieterin sowie die Portnummer;
  - den Typ des Transportprotokolls, z.B. TCP (*Bst. e*);
  - den Zeitpunkt der NAT-Operation nach Datum und Uhrzeit (*Bst. f*).
  - Falls für die Identifikation notwendig (hängt vom NAT-Verfahren ab), muss das Auskunftsgesuch die öffentliche Ziel-IP-Adresse und Ziel-Portnummer (*Bst. c und d*) des Zielservers enthalten.

Beispiel zu Abfragemöglichkeit 1: Wenn der Auskunftstyp IR_4_IP (NAT) nach Artikel 36 nicht zum Erfolg führt, muss die Quell-IP-Adresse möglicherweise weiter rückverfolgt werden, um letztendlich die Benutzerschaft zu identifizieren. Dieser Prozess wird als "Backtracking" (Rückverfolgung) bezeichnet. Das "Backtracking" ist nur möglich, wenn jede der beteiligten Mitwirkungspflichtigen präzise und vollständig alle für die Identifikation notwendigen Informationen ihrer NAT-Übersetzungen speichert. Welche Informationen dies im Einzelnen sind, hängt von den Verfahren ab, welche die Mitwirkungspflichtige verwendet. Beim Backtracking ist auch ein mehrstufiges Verfahren möglich (von NAT zu NAT), das heisst Anfragen an alle Mitwirkungspflichtigen, die für die gesuchte Internet-Verbindung eine NAT-Übersetzung durchgeführt haben.

Beispiel zu Abfragemöglichkeit 2: Im Rahmen einer Echtzeitüberwachung des Netzzugangs wird festgestellt, dass die überwachte Person einen bestimmten abgeleiteten Kommunikationsdienst benutzt. Die Daten werden jedoch verschlüsselt übertragen, so dass der Benutzeridentifikator des abgeleiteten Kommunikationsdienstes bei der Netzzugangsüberwachung nicht sichtbar ist. Die Strafverfolgungsbehörde möchte nun den Benutzeridentifikator herausfinden. Bei der Anbieterin des abgeleiteten Kommunikationsdienstes ist jedoch aufgrund der NAT-Operation der Zugangsanbieterin eine andere (öffentliche) Quell-IP-Adresse sichtbar, als die der überwachten Person zugeteilte (private) IP-Adresse, welche der Strafverfolgungsbehörde aufgrund der Randdaten der Echtzeitüberwachung bekannt ist. Um den fraglichen Zugriff bei der Anbieterin des abgeleiteten Kommunikationsdienstes identifizieren zu können, kann die gesuchte öffentliche Quell-IP-Adresse und die Quell-Portnummer unter Angabe der bekannten IP-Verbindungsdaten bei der Zugangsanbieterin mittels dieses Auskunftstyps abgefragt werden.

5. Abschnitt: Auskunftstypen für Anwendungen

Art. 38 Auskunftstyp IR_6_TEL: Auskünfte über Teilnehmende von Telefonie- und Multimediadiensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von Telefonie- und Multimediadiensten. Dieser Auskunftstyp entspricht im Prinzip den bisherigen Auskünften A0 und teilweise A1 (Abs. 2 Bst. j und k). Neu sind Abfragen nach der Unternehmens-Identifikationsnummer (Abs. 2 Bst. g), dem Teilnehmeridentifikator (Abs. 2 Bst. h) und dem Dienstidentifikator (Abs. 2 Bst. l).

Zu den Telefonie- und Multimediadiensten zählen insbesondere die klassischen analogen und digitalen Telefoniedienste im Festnetz (zum Beispiel POTS, ISDN), die mobilen Telefoniedienste inklusive SMS und Voice Mail (zum Beispiel GSM, UMTS), die Internet-Telefonie (zum Beispiel VoIP), die Multimedia-Telefoniedienste des IMS (zum Beispiel VoLTE, VoWLAN, Präsenz, RCS), die Videotelefonie und die Konferenzschaltungen.

Dieser Auskunftstyp basiert auf dem ETSI-Standard TS 102 657 und kombiniert die allgemeinen Teilnehmerinformationen (generic subscriber info) mit den wichtigsten Angaben zu den Telefonie- und Multimediadiensten des Teilnehmenden. Weitere spezifische Angaben über Telefonie- und Multimediadienste können über den Auskunftstyp IR_7_TEL (Art. 39) abgefragt werden.

Artikel 38 gilt sowohl für Abonnements- als auch für Prepaid-Verhältnisse. Dieser Auskunftstyp ist analog zu Artikel 33 aufgebaut, weshalb die dortigen Erläuterungen auch für diese Bestimmung gelten.

Ähnlich wie bei Artikel 33 Absatz 1 hält *Absatz 1* fest, welche Angaben im Falle einer Auskunft über Teilnehmende von Telefonie- und Multimediadiensten zu liefern sind. Die Angaben zum Typ des Dienstes (*Ziff. 4*) dienen zur näheren Beschreibung des Dienstes. Bei den Standortangaben des Festnetzzugangs und jeweils deren Gültigkeitszeitraum (*Ziff. 5*) sind, soweit es sich um einen Telefonie - und Multimediadienst im Festnetz handelt, die bei der Anbieterin registrierten Angaben zu liefern (z.B. Adresse des Standorts). Da sich der Standort im Laufe der Kundenbeziehung ändern kann, ist die gesamte bekannte Historie zu liefern, jeweils mit Beginn- und End-Datum (soweit zutreffend). Bei diesen Angaben kann jedoch nicht immer garantiert werden, dass sie mit dem tatsächlichen Standort des Zugangs übereinstimmen, da der Teilnehmende bei manchen Dienstangeboten die entsprechenden Zugangsgeräte auch ohne Wissen der Anbieterin an einem anderen Standort betreiben kann.

Anzugeben hat die Anbieterin ausserdem, soweit zutreffend, die Liste beziehungsweise den Bereich der weiteren im Zusammenhang mit dem Telefonie- oder Multimediadiensten registrierten Adressierungselemente (*Ziff. 7*) sowie falls zutreffend, die Angaben zur vorbestimmten freien Wahl der Anbieterin für Verbindungen (*Ziff. 9*). Unter den Angaben zur vorbestimmten freien Wahl der Dienstanbieterin für Verbindungen ist der voreingestellte (pre-selected) Carrier Selection Code zu verstehen. Gemäss Artikel 9 Absatz 1 der Verordnung der

Eidgenössischen Kommunikationskommission vom 17. November 1997[40] betreffend das Fernmeldegesetz müssen die Anbieterinnen öffentlicher Telefoniedienste über ein Festnetz ihren Teilnehmenden die Möglichkeit bieten, eine Anbieterin für nationale und internationale Verbindungen zu wählen, und zwar sowohl vorbestimmt als auch für jeden einzelnen Anruf. Falls die vorbestimmte Wahl der Anbieterin für nationale und internationale Verbindungen bekannt ist, hat die Anbieterin des Telefoniedienstes über ein Festnetz diese Information im Rahmen des Auskunftsgesuches mitzuteilen.

Auch *Absatz 2* hält ähnlich wie Artikel 33 Absatz 2 die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (siehe die entsprechenden Erläuterungen zu Art. 33 Abs. 2).

Bei den Anfragekriterien wird zwischen Identifikatoren (Bst. h, j, k und l) und Adressierungselementen (Bst. i) unterschieden. Die Identifikatoren bestimmen eindeutig bestimmte Telefonie- und Multimediadienste, dienen aber im Gegensatz zu den Adressierungselementen nicht zur Adressierung beim Kommunikationsaufbau. Identifikatoren wie IMSI oder IMPI dienen zur Identifizierung des Teilnehmenden gegenüber dem Netz und werden von den Anbieterinnen hochvertraulich behandelt.

Da eine Anbieterin gestützt auf Artikel 23 der Verordnung vom 6. Oktober 1997[41] über die Adressierungselemente im Fernmeldebereich (AEFV) Telefonnummern aus einem ihr zugeteilten Nummernblock weiter zuteilen kann (sog. untergeordnete Zuteilung einer Telefonnummer), sind bei dieser Anbieterin in der Regel für die untergeordnet zugeteilten Telefonnummern keine aktuellen Teilnehmerdaten vorhanden. In diesem Fall hat diese Anbieterin in ihrer Antwort die untergeordnete Zuteilung sowie den Namen und die Kontaktdaten (Adresse, Telefonnummer) derjenigen Anbieterin anzugeben, an welche die abgefragte Telefonnummer weiter zugeteilt wurde.

Art. 39 Auskunftstyp IR_7_TEL: Auskünfte über Telefonie- und Multimediadienste

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Telefonie- und Multimediadienste. Dieser Auskunftstyp entspricht im Prinzip der bisherigen Auskunft A1 (technische Daten). Der Begriff *Telefonie- und Multimediadienste* wird bei Artikel 38 erläutert.

Absatz 1 hält ähnlich wie Artikel 34 Absatz 1 fest, welche Angaben im Falle einer Auskunft über Telefonie- und Multimediadienste zu liefern sind. Bei der Liste der Geräteidentifikatoren (*Bst. d*) ist zu beachten, dass die Liste der im Anfragezeitraum tatsächlich benutzten Geräteidentifikatoren zu liefern ist. Diese Informationen hat die Anbieterin aus den aufbewahrten Randdaten zu gewinnen, ohne jedoch die Randdaten selbst herauszugeben. Das heisst, aus der Antwort darf nicht ersichtlich sein, wann, wie und wo die Benutzung der Geräte im Einzelnen stattgefunden hat. Zu liefern ist also beispielsweise eine Liste der IMEI der im Auftragszeitraum tatsächlich benutzten Mobilfunkgeräte (egal wie lange die Benutzung gedauert hat), ohne Angabe, wann genau die Endgeräte benutzt wurden.

40 SR **784.101.112**
41 SR **784.104**

Die Aufbewahrungsdauer für die tatsächlich benutzten Geräteidentifikatoren (z.B. MAC-Adressen, IMEI) ist auf 6 Monate beschränkt, da es sich hierbei um Randdaten im Sinne von Artikel 26 BÜPF handelt (Art. 21 Abs. 2 2. Satz und 22 Abs. 2 2. Satz und Abs. 4 BÜPF sowie Art. 20 Abs. 2).

Auch *Absatz 2* hält ähnlich wie Artikel 34 Absatz 2 die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (siehe die entsprechenden Erläuterungen zu Art. 34 Abs. 2).

Bei den Anfragekriterien wird zwischen Adressierungselementen (*Bst. a*) und Identifikatoren (*Bst. b*, *c* und *e*) unterschieden.

Art. 40 Auskunftstyp IR_8_EMAIL: Auskünfte über Teilnehmende von E-Mail- Diensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von E-Mail-Diensten. Dieser Auskunftstyp entspricht im Prinzip den bisherigen Auskünften A0 und teilweise A1.

Dieser Auskunftstyp ist analog zu Artikel 38 aufgebaut, weshalb die dortigen Erläuterungen auch für diese Bestimmung gelten. Ähnlich wie beim Artikel 38 Absatz 1 hält *Absatz 1* fest, welche Angaben im Falle einer Auskunft über Teilnehmende von E-Mail-Diensten zu liefern sind.

Unter den anzugebenden weiteren Adressierungselementen, die zum betreffenden Dienst gehören (*Bst. c Ziff. 4*) sind zum Beispiel Alias-Adressen zu verstehen. Alias-Adressen sind zusätzliche E-Mail-Adressen, die zum selben E-Mail-Postfach gehören. Der Teilnehmende kann diese beliebig einrichten, ändern oder löschen. Deren maximale Anzahl und Aufbau werden von der E-Mail-Anbieterin vorgegeben. Die Alias-Adressen sind mit dem betreffenden E-Mail-Postfach verknüpft. An eine Alias-Adresse gesendete E-Mails werden in das gleiche E-Mail-Postfach der zugehörigen Haupt-E-Mail-Adresse des Teilnehmenden zugestellt.

Eine nach *Ziffer 5* anzugebende Adresse ist zum Beispiel eine Mailingliste. Die Mailingliste ist eine Liste von E-Mail-Adressen und wird auch als Verteilerliste oder Verteilergruppe bezeichnet. Die Mailingliste besitzt selbst eine E-Mail-Adresse. Die Nachrichten, die an die Adresse der Mailingliste geschickt werden, werden an die E-Mail-Adressen ihrer Mitglieder weitergeleitet. Der Teilnehmende kann auch E-Mails mit der Adresse der Mailingliste als Absender verschicken.

Unter den weiteren Adressierungselementen nach *Buchstabe d* sind andere E-Mail-Adressen oder Telefonnummern zu verstehen, die mit dem betreffenden Dienst an und für sich nichts zu tun haben. Diese alternativen Adressierungselemente werden zum Beispiel verwendet, um das Passwort zurückzusetzen oder Sicherheitsmeldungen an den Teilnehmenden zu senden.

Absatz 2 hält ähnlich wie Artikel 38 Absatz 2 die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (siehe die entsprechenden Erläuterungen zu Art. 38 Abs. 2).

Art. 41 Auskunftstyp IR_9_COM: Auskünfte über Teilnehmende von anderen Fernmelde- oder abgeleiteten Kommunikationsdiensten

Diese Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über Teilnehmende von anderen Fernmelde- oder abgeleiteten Kommunikationsdiensten. Auch dieser Auskunftstyp entspricht im Prinzip den bisherigen Auskünften A0 und teilweise A1, wird aber neu für diese Kategorie von Diensten eingeführt. Durch diese Bestimmung sollen alle Fernmelde- oder abgeleiteten Kommunikationsdienste erfasst werden können, die zwar bereits in Betrieb sind, für welche die entsprechenden ETSI-Standards jedoch erst in Bearbeitung stehen. Die Bestimmung soll auch als Auffangtatbestand für alle weiteren, durch den technischen Fortschritt zu erwartenden Dienste dienen. Als Beispiel können die Kommunikationsdienste in sozialen Netzen, Cloud- und Proxy-Dienste aufgeführt werden. Cloud-Dienste sind abgeleitete Kommunikationsdienste wie verteilte Speicherdienste und Applikationen, die über das Internet angeboten werden. Diese sind online verfügbar und je nach Ressourcenbedarf in verteilten Rechenzentren beherbergt. Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen. Proxy-Dienste sind daher für die Identifikation der Benutzerschaft bei Straftaten über das Internet relevant.

Ebenso in diese Kategorie gehören die Mitteilungsdienste, welche eigenständige (d.h. unabhängig von Telefonie- und Multimediadiensten angebotene) hauptsächlich asynchrone Dienste zur Übermittlung von Mitteilungen oder Nachrichten sind. Dazu gehören unter anderem Instant Messaging, IMS Messaging, Messaging Applikationen (Apps) und SMS von Drittanbieterinnen (d.h. SMS-Dienste, die nicht von der FDA des Teilnehmenden erbracht werden). Diese Dienste können auch erweiterte Zusatzfunktionen enthalten wie Multimediakommunikation, Dateiübertragung und Präsenzinformationen (z.B. der Teilnehmende kann den aktuellen Status und eventuell den Standort der anderen Teilnehmenden sehen).

Dieser Artikel ist gleich aufgebaut wie die Artikel 38-40. Aus diesem Grund kann auf die Erläuterungen zu letzteren Bestimmungen verwiesen werden.

Absatz 1 hält fest, welche Angaben im Falle einer Auskunft über Teilnehmende von Telefonie- und Multimediadiensten zu liefern sind.

Absatz 2 hält, ähnlich wie in Artikel 38-40, die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind (siehe die entsprechenden Erläuterungen zu Art. 38 Abs. 2).

6. Abschnitt: Weitere Auskunftstypen

Art. 42 Auskunftstyp IR_10_PAY: Auskünfte über die Zahlungsweise der Teilnehmenden von Fernmelde- und abgeleiteten Kommunikationsdiensten

Die Bestimmung definiert den standardisierten Auskunftstyp für Auskünfte über die Zahlungsweise der Teilnehmenden von Fernmelde- und abgeleiteten Kommunikationsdiensten. Da sich die Zahlungsweise nicht wesentlich zwischen den einzelnen Dienstkategorien unterscheidet, werden mit diesem Auskunftstyp alle Dienstkategorien abgedeckt. Dieser Auskunftstyp basiert auf dem ETSI-Parameter PaymentDetails.

Für die bisherige Auskunft A1 (technische Daten) über verwendete Aufladecodes (auch Rubbelcodes oder Scratch Codes genannt) für Prepaid-Dienste gibt es noch keinen geeigneten ETSI-Parameter. Neu erfolgt eine Ausweitung der mit diesem Auskunftstyp einholbaren Auskünfte auf alle Arten von Zahlungsweisen im Zusammenhang mit Fernmelde- beziehungsweise abgeleiteten Kommunikations-diensten, unabhängig davon, ob es sich um Prepaid- oder abonnierte Dienste handelt.

Absatz 1 hält fest, welche Angaben zu liefern sind.

Absatz 2 hält fest, dass nur diejenigen Daten geliefert werden müssen, die bei den Anbieterinnen vorhanden sind. Beispielsweise sind bei Gratisdiensten wie E-Mail keine Informationen über die Zahlungsweise nötig und demzufolge nicht vorhanden. *Absatz 3* hält die einzelnen Anfragekriterien für diesen Auskunftstyp fest und gibt vor, wie die Anfragekriterien bei diesem Auskunftstyp zu verwenden sind.

Art. 43 Auskunftstyp IR_11_ID: Ausweiskopie

Welche Angaben zur Person sowohl beim Verkauf von Prepaid-Karten als auch bei Abonnementsabschlüssen und bei Gratisangeboten zu erfassen sind, wird in Artikel 19 geregelt. Damit die Korrektheit der erfassten Angaben gewährleistet werden kann sowie um Falschregistrierungen vorzubeugen, wird unter anderem verlangt, dass die betreffende Mitwirkungspflichtige auch eine elektronische Kopie des Ausweises des betreffenden Teilnehmenden hinterlegt. Wie die betreffende Mitwirkungspflichtige die elektronische Kopie hinterlegt, wird nicht vorgeschrieben. Vorausgesetzt wird lediglich, dass die hinterlegte elektronische Kopie des Ausweises gut lesbar und die Mitwirkungspflichtige in der Lage ist, diese auf Anfrage hin zu liefern. Die anordnende Behörde hat dabei im Auskunftsgesuch zu präzisieren, auf welchen Zeitraum und auf welchen eindeutigen Teilnehmer- oder Dienstidentifikator sich die Anfrage bezieht (*Abs. 2*). Die Ausweiskopie ist auf elektronischem Wege zu liefern.

Art. 44 Auskunftstyp IR_12_BILL: Rechnungskopie

Dieser Auskunftstyp entspricht der bisherigen Auskunft A2 (Rechnungsdaten) (siehe insbesondere Art. 21 Abs. 1 Bst. d BÜPF). Die Mitwirkungspflichtige muss eine elektronische Kopie der vorhandenen Rechnungsunterlagen des Teilnehmenden liefern. Wichtig ist, dass dabei keinerlei Randdaten mitgeliefert werden. Beispielsweise dürfen keine Verbindungen auf der Rechnungskopie

erscheinen. Es genügt zum Beispiel, jeweils die erste Seite (Zusammenfassung) der Monatsrechnungen zu übermitteln, welche den Rechnungsbetrag, die Kundennummer und die Rechnungsadresse enthält. Die anfragende Behörde hat in ihrem Auskunftsgesuch zu präzisieren, auf welchen Zeitraum und auf welchen eindeutigen Teilnehmer- oder Dienstidentifikator sich die Anfrage bezieht (*Abs. 2*).

Art. 45 Auskunftstyp IR_13_CONTRACT: Vertragskopie

Dieser Auskunftstyp entspricht der bisherigen Auskunft A2 (Vertragskopie) (siehe insbesondere Art. 21 Abs. 1 Bst. d BÜPF). Im Falle einer Auskunftsanfrage ist eine elektronische Kopie der vorhandenen Vertragsunterlagen oder von vergleichbaren Aufzeichnungen zu liefern. Da Verträge sowohl schriftlich als auch mündlich abgeschlossen werden können, kann es vorkommen, dass kein schriftlicher Vertrag vorhanden ist. Durch diese Bestimmung wird keine Verpflichtung für die Mitwirkungspflichtigen eingeführt, nur noch schriftliche Verträge abschliessen zu müssen. Sollte kein schriftlicher Vertrag vorhanden sein, genügt es, dass die Mitwirkungspflichtige zum Beispiel eine Bildschirmkopie aus ihrem System liefert, welche über die Vertragsbeziehung Auskunft gibt. Die anordnende Behörde hat in ihrem Auskunftsgesuch zu präzisieren, auf welchen Zeitraum und auf welchen eindeutigen Teilnehmer- oder Dienstidentifikator sich die Anfrage bezieht (*Abs. 2*).

Art. 46 Auskunftstyp IR_14_TECH: Technische Daten

Dieser Artikel hält fest, dass die Mitwirkungspflichtigen die technischen Daten von Fernmeldesystemen und Netzelementen zu liefern haben (siehe insbesondere Art. 21 Abs. 1 Bst. d BÜPF). Dieser Auskunftstyp entspricht der bisherigen Auskunft A3.

In *Absatz 1* werden beispielhaft einige typische technische Daten aufgeführt. Zu den technischen Daten von Fernmeldesystemen und Netzelementen gehören auch Angaben über nicht an einen festen Standort gebundene Mobilfunkantennen oder WLAN-Zugangspunkte, beispielsweise in Flugzeugen (Fluggesellschaft, Luftfahrzeugkennzeichen), Zügen (Bahnunternehmen und Zugnummer), Bussen (Busunternehmen und Busnummer) oder an Bord von Kreuzfahrtschiffen (Reederei, Schiffsname).

Was die Standortangaben von Mobilfunkzellen und WLAN-Zugangspunkten umfasst, regelt *Absatz 2* diese näher. Die Angaben nach *Buchstabe b–d* sind nur zu liefern, sofern solche vorhanden sind.

Absatz 3 hält die einzelnen Anfragekriterien für diesen Auskunftstyp fest und schreibt vor, dass das Auskunftsgesuch mindestens eines der erwähnten Kriterien enthalten muss. Zudem hat die anordnende Behörde in ihrem Auskunftsgesuch zu präzisieren, auf welchen Zeitraum sich die Anfrage bezieht und welche Angaben gemäss Absatz 1 gewünscht sind. Bei Anfragen anhand der geografischen Koordinaten (*Bst. a*) sind diese mit hinreichender Genauigkeit anzugeben und beziehen sich auf genau einen Standort von Netzelementen. Die Anbieterin hat die gewünschten Angaben zu allen Netzelementen zu liefern, die sich am angefragten Standort befinden. Die Anbieterin muss jedoch keine Abdeckungsanalyse für die in der Anfrage angegebenen geografischen Koordinaten durchführen. Für Abdeckungsanalysen dient der Überwachungstyp AS_27_PREP_COV (Art. 64).

7. Abschnitt: Allgemeine Bestimmungen für die Überwachung des Fernmeldeverkehrs

Art. 47 Anordnung zur Überwachung des Fernmeldeverkehrs

Diese Bestimmung entspricht im Wesentlichen dem Artikel 15 der VÜPF vom 31. Oktober 2001[42] und regelt den Inhalt der Überwachungsanordnung im Falle einer Überwachung des Fernmeldeverkehrs (für den Postverkehr, siehe oben die Erläuterungen zu Art. 15). Mit Ausnahme der Zugriffsrechte kann eine bereits quittierte Überwachungsanordnung nicht mehr geändert werden. Wesentliche Änderungen einer Überwachungsanordnung wie Überwachungstyp und Zielidentifikator erfordern eine neue Überwachungsanordnung. Die Neuanordnung unterliegt den üblichen Gebühren und Entschädigungen.

Absatz 1 führt abschliessend diejenigen Angaben auf, welche die Überwachungsanordnung enthalten muss.

Buchstabe a: Der Dienst ÜPF prüft formell, ob diese Behörde zur Anordnung dieser Überwachung berechtigt ist.

Buchstabe b: Gemäss diesen Angaben erteilt der Dienst ÜPF den aufgeführten Personen die Zugriffsrechte im Verarbeitungssystem zu den Überwachungsdaten dieser Überwachung.

Buchstabe c: Falls vorhanden, dienen diese Angaben zur Kontrolle bei der FDA beziehungsweise der Anbieterin abgeleiteter Kommunikationsdienste, ob die zu überwachende Anwendung beziehungsweise der zu überwachende Internetzugang mit dieser Person in Zusammenhang stehen.

Buchstabe d: Die Referenznummer und der Fallname ist für die korrekte Erfassung im Verarbeitungssystem notwendig.

Buchstabe e: Der Dienst ÜPF prüft formell, ob diese Straftat beziehungsweise Straftaten die Anordnung dieser Überwachung gemäss Katalog im Artikel 269 StPO oder gemäss Artikel 273 StPO erlaubt, beziehungsweise erlauben.

Buchstabe f: Die anordnende Behörde teilt dem Dienst ÜPF den Namen der Mitwirkungspflichtigen mit, welche die Überwachung durchzuführen hat.

Unter *Buchstabe g* sind die angeordneten Überwachungstypen aufgeführt. Es können sowohl standardisierte als auch nicht-standardisierte Überwachungstypen angeordnet werden. Bei Unklarheiten, Widersprüchen oder zu erwartenden hohen Gebühren nimmt der Dienst ÜPF Rücksprache mit der anordnenden Behörde.

Buchstabe h: Die anordnende Behörde teilt dem Dienst ÜPF die zu überwachenden Adressierungselemente mit. Bei Unklarheiten nimmt der Dienst ÜPF Rücksprache mit der anordnenden Behörde.

Buchstabe i: Falls die zu überwachende Person in rascher Folge den Fernmeldeanschluss wechselt, kann das Zwangsmassnahmengericht gemäss Artikel 272 Abs. 2 StPO mittels Rahmenbewilligung die Überwachung aller identifizierten Anschlüsse bewilligen, über welche die zu überwachende Person ihren Fernmeldeverkehr abwickelt, ohne dass jedes Mal eine Genehmigung im Einzelfall

42 SR **780.11**

nötig ist. Der Antrag auf Rahmenbewilligung ist der Überwachungsanordnung beizulegen.

Buchstabe j: Die anordnende Behörde muss angeben, in welchem Zeitraum die Überwachung durchgeführt werden soll. Es sind hierbei die geltenden Fristen zu berücksichtigen. So können Echtzeitüberwachungen lediglich für maximal drei Monate in die Zukunft und rückwirkende Überwachungen lediglich für maximal sechs Monate in die Vergangenheit angeordnet werden.

Für die *Buchstaben k* und *l*, siehe die Erläuterungen zu Artikel 5. Dies ist die Kennzeichnung, dass diese Überwachung Personen betrifft, die einem Amts- oder Berufsgeheimnis nach Artikel 271 der Strafprozessordnung (StPO) oder 70b MStP wie Rechtsanwälte und Ärzte unterstehen. Der Dienst ÜPF hat für diese Überwachung die Triage der Aufzeichnung der erhaltenen Daten während einer Überwachung einer dem Amts- oder Berufsgeheimnis unterstellten Person vorzubereiten.

Absatz 2 bezieht sich auf Überwachungen, für deren Durchführung weitere technische Angaben erforderlich sind, beispielsweise weil der Überwachungstyp nicht standardisiert ist oder weil die Ausleitung der Überwachungsdaten nicht auf das Verarbeitungssystem des Dienstes ÜPF erfolgt.

Art. 48 Überwachungspflichten

Absatz 1 definiert den Kreis der Mitwirkungspflichtigen, die mit Überwachungen des Fernmeldeverkehrs beauftragt werden können. Einen Auftrag zur aktiven Überwachung im Bereich des Fernmeldeverkehrs können wie bisher die Anbieterinnen von Fernmeldediensten sowie neu die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten nach Artikel 50 erhalten. Neu wird in der Verordnung auch festgehalten, dass Anbieterinnen von Fernmeldediensten mit reduzierten Überwachungspflichten nicht Adressat eines solchen Überwachungsauftrages sein können. Es handelt sich dabei um die Überwachungspflichten nach dem 3. Kapitel Abschnitt 8–12. Nach der Bestimmung müssen die betreffenden Mitwirkungspflichtigen in der Lage sein, die erwähnten Pflichten entweder selber auszuführen oder durch einen Dritten ausführen zu lassen (Art. 32 BÜPF).

Nach *Absatz 2* ist die Überwachungsbereitschaft von der Aufnahme des Kundenbetriebes eines Dienstes an sicherzustellen. Dies bedeutet, dass das Abnahmeverfahren zur Überprüfung der Auskunfts- und Überwachungsbereitschaft vorgängig durchgeführt und erfolgreich abgeschlossen werden muss (vgl. Ausführungen zu den Art. 29-32).

Absatz 3 weist darauf hin, dass Überwachungsaufträge sowohl innerhalb als auch ausserhalb der Normalarbeitszeiten (siehe Art. 10) entgegengenommen und innerhalb der vorgegebenen Frist ausgeführt werden müssen. Die Festlegung der Fristen für die Ausführung der Überwachungsaufträge wird an das EJPD delegiert. Das EJPD regelt diese Fristen in der Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF).

Absatz 4 regelt, in welchem Zeitraum welcher Teil des Fernmeldeverkehrs zu überwachen ist. Der Dienst ÜPF teilt der Mitwirkungspflichtigen den durch die anordnende Behörde in der Überwachungsanordnung bestimmten Zeitraum der Überwachung mit, indem er bei Echtzeitüberwachungen einen Aktivierungsauftrag

zum Beginn der Überwachung und einen Deaktivierungsauftrag zu deren Ende sendet. Bei rückwirkenden Überwachungen wird nur ein Aktivierungsauftrag gesendet, der den Überwachungszeitraum angibt. Bei Echtzeitüberwachungsaufträgen weiss die Mitwirkungspflichtige beim Eingang des Aktivierungsauftrages noch nicht, wann die Echtzeitüberwachung enden wird. Das Ende der Überwachung wird der Mitwirkungspflichtigen erst mit dem Deaktivierungsauftrag mitgeteilt.

Die Mitwirkungspflichtige muss grundsätzlich sicherstellen, dass jeglicher von ihr kontrollierter Fernmeldeverkehr überwacht werden kann. Ausgeleitet werden muss aber nur derjenige Fernmeldeverkehr, der an den überwachten Netzzugang gerichtet ist beziehungsweise von diesem stammt oder der mit der überwachten Anwendung beziehungsweise dem überwachten Zielidentifikator (z.B. Telefonnummer eines Telefoniedienstes) im Zusammenhang steht (z.B. Anrufe von oder zu dieser Telefonnummer). Der Begriff "der von ihr kontrollierte Fernmeldeverkehr" umfasst die Infrastruktur, welche die Mitwirkungspflichtige besitzt, mietet, verwaltet, ausgelagert hat (Outsourcing) oder in einem besonderen Nutzungsrecht (z.B. MVNO) vertraglich nutzt. Bei der Benutzung *ausländischer* Infrastruktur (z.B. Roaming im Ausland) ist der Fernmeldeverkehr nur insoweit zu überwachen, wie er von der Mitwirkungspflichtigen im Rahmen des üblichen technischen Betriebs kontrolliert werden kann. Bei der Benutzung fremder *inländischer* Infrastruktur, zum Beispiel nationales Roaming, Mobile Virtual Network Operator (MVNO), hat die Mitwirkungspflichtige sicherzustellen, dass der gesamte zu überwachende Fernmeldeverkehr von ihr oder von Dritten ausgeleitet wird.

Eine Mitwirkungspflichtige muss also auch in der Lage sein, Fernmeldeverkehr zu überwachen, welcher Adressierungselemente betrifft, die sie nicht vergeben hat oder die sich nicht in ihrem Netz befinden beziehungsweise nicht in ihrem Netz eingebucht sind (z.B. Überwachung einer ausländischen Telefonnummer - siehe Art. 69).

Beim Roaming gibt es zwei Szenarien.

1. Outbound Roaming: Überwachung eines eigenen Teilnehmenden der beauftragten Anbieterin, wenn dessen Endgerät als Besucher in einem fremden Netz eingebucht ist. Beim Outbound Roaming werden zwei Szenarien unterschieden:

A) fremdes Netz im Inland

B) fremdes Netz im Ausland

Die beiden Szenarien unterscheiden sich dadurch, dass im Szenario A die beauftragte Anbieterin dafür sorgen muss, dass der gesamte Fernmeldeverkehr ihrer Teilnehmenden von ihr oder von Dritten auch dann überwacht wird, wenn sie das fremde Netz im Inland benutzen.

Im Szenario B dagegen muss die beauftragte Anbieterin lediglich diejenigen Randdaten und Kommunikationsinhalte überwachen können, die sie im Rahmen der üblichen Betriebsverfahren (Routing, Signalisierung, siehe auch Art. 52 Abs. 1 Bst. h) kontrolliert und auf die sie demzufolge zugreifen kann.

2. Inbound Roaming: Überwachung eines fremden Teilnehmenden, dessen Endgerät als Besucher im Netz der beauftragten Mitwirkungspflichtigen eingebucht ist. In diesem Szenario ist die Überwachung möglich, da sich der

fremde Teilnehmende im Netz der beauftragten Mitwirkungspflichtigen befindet. Aufgrund bestimmter technischer Besonderheiten kann es jedoch vorkommen, dass die Kommunikationsinhalte nur verschlüsselt ausgeleitet werden können, wenn beispielsweise die Daten verschlüsselt in einem Tunnel zwischen dem fremden Teilnehmenden und dessen Heimnetzwerk übertragen werden, dessen Verschlüsselung die beauftragte Mitwirkungspflichtige nicht angebracht hat und daher auch nicht entfernen kann. Dagegen hat beispielsweise eine ausländische Mobilfunkanbieterin, die nicht als Mitwirkungspflichtige im Sinne des Art. 2 BÜPF gilt und deren Kunden lediglich als Inbound-Roamer in einem Schweizer Netz eingebucht sind, keine Pflichten nach dem BÜPF.

Die übermittelten Überwachungsdaten müssen mit dem im Überwachungsauftrag bezeichneten Fernmeldeverkehr übereinstimmen. Dabei muss die Mitwirkungspflichtige den Dienst ÜPF bei Bedarf unterstützen (vgl. *Abs. 5*).

Gemäss *Absatz 6* muss die Mitwirkungspflichtige des Weiteren sicherstellen, dass, falls weitere Identifikatoren mit dem Zielidentifikator assoziiert sind, auch diese im Rahmen des Überwachungstyps überwacht werden.

Zum Schluss hält *Absatz 7* fest, dass die Überwachungsdaten einer bereits begonnenen Kommunikation zum Zeitpunkt der Aktivierung einer Echtzeitüberwachung unverzüglich zu liefern sind.

Art. 49 FDA mit reduzierten Überwachungspflichten

FDA müssen grundsätzlich in der Lage sein, die Überwachungspflichten, die durch sie angebotene Dienste betreffen, auszuführen oder durch Dritte ausführen zu lassen (Art. 32 BÜPF). Dies bedeutet für die FDA unter anderem, dass sie über die für die Fernmeldeüberwachung erforderlichen Einrichtungen und verfügen müssen. Die Beschaffung der erforderlichen Einrichtungen ist mit Investitionskosten verbunden, die nicht von allen FDA gleich gut getragen werden können. Dies wird vor allem von den kleinen und mittelgrossen FDA negativ wahrgenommen. Deshalb hat der Gesetzgeber in Artikel 26 Absatz 6 BÜPF dem Bundesrat die Kompetenz eingeräumt, FDA, die Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten, von bestimmten gesetzlichen Pflichten zu befreien. Nicht befreit werden können diese Anbieterinnen jedoch von der gesetzlichen Minimalpflicht, eine Überwachungsmassnahme zu dulden, angebrachte Verschlüsselungen zu entfernen, Zugang zu ihren Anlagen zu gewähren sowie die vorliegenden Randdaten des Fernmeldeverkehrs der überwachten Person zu liefern (Art. 26 Abs. 2 BÜPF).

Absatz 1 konkretisiert die einzelnen Voraussetzungen, welche bestehen müssen, damit eine FDA keine weiteren als die gesetzliche Minimalpflicht zu erfüllen hat. Eine FDA hat dann reduzierte Überwachungspflichten, wenn sie ihre Fernmeldedienste nur im Bildungsbereich anbietet oder beide der folgenden Grössen nicht erreicht: 10 Überwachungsaufträge in den letzten 12 Monaten erhalten (wobei der 30. Juni als Stichtag dient) und einen Jahresumsatz von weniger als 100 Millionen Franken in zwei aufeinander folgenden Geschäftsjahren erzielt. Das letzte Kriterium wird dadurch weiter eingeschränkt, dass nur der mit Fernmelde- und abgeleiteten Kommunikationsdiensten erzielte Jahresumsatz in Betracht gezogen wird. FDA, welche ihre Dienstleistungen ausschliesslich im Bildungsbereich anbieten, haben rein aufgrund der Tatsache, dass sie nur im Bildungsbereich tätig sind, lediglich die gesetzliche Minimalpflicht zu erfüllen.

Wir gehen davon aus, dass sich aufgrund der Anwendung der Schwellenwerte nach Buchstabe b die Anzahl der nach bisherigem Recht aktiv überwachungspflichtigen FDA von rund 450 auf etwa 20 bis 50 FDA verringern wird. Auf jeden Fall wird diese Befreiung von bestimmten Überwachungspflichten in der Praxis keine Lücken bei der Fernmeldeüberwachung zur Folge haben. Die Überwachungen können auch bei FDA mit reduzierten Überwachungspflichten durchgeführt werden, da diese Anbieterinnen immer eine Duldungs- und Zusammenarbeitspflicht haben und der Dienst ÜPF die nötigen Schritte unternimmt, damit die Überwachungen dennoch durchgeführt werden können (Art. 17 Bst. e BÜPF).

Der Konzerntatbestand nach *Absatz 2* beschreibt wie beim Artikel 21 den Fall, bei dem ein oder mehrere rechnungspflichtige Unternehmen von einer FDA kontrolliert werden. Wie beim Artikel 21 werden auch in diesem Fall die beteiligten Unternehmen und die betreffende FDA als eine Einheit betrachtet. Dadurch sollen Missbrauchsfälle verhindert werden (für weitere Ausführungen siehe Art. 21).

Sollten sich die Schwellenwerte nach Absatz 1 ändern oder eine FDA ihre Dienstleistungen nicht mehr ausschliesslich im Bildungsbereich anbieten, hat die betreffende FDA dies dem Dienst ÜPF innert drei Monaten nach Abschluss ihres Geschäftsjahres mitzuteilen und entsprechende Belege einzureichen (*Absatz 3*).

Kommt der Dienst ÜPF nach Einsicht in die Unterlagen zum Schluss, dass die FDA die Voraussetzungen nach Absatz 1 erfüllt, teilt sie dies der betreffenden FDA mit. Die Überwachungsbereitschaft entfällt ab dem Zeitpunkt der Mitteilung (*Absatz 4*).

Wie beim Artikel 21 Absatz 4 hat die FDA die Speicherung der für die Überwachung erforderlichen Daten innert 2 Monaten und die Überwachungsbereitschaft innert 12 Monaten sicherzustellen, sobald ihr der Dienst ÜPF bestätigt, dass sie nicht mehr als FDA mit reduzierten Überwachungspflichten gilt (*Absatz 5*).

Der Dienst ÜPF trifft die notwendige Entscheide (*Absatz 6*).

Art. 50 Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten

Ähnlich wie bei den Auskunftspflichten nach Artikel 22 BÜPF hat der Gesetzgeber in Artikel 27 Absatz 3 BÜPF dem Bundesrat die Kompetenz eingeräumt, den Anbieterinnen abgeleiteter Kommunikationsdienste weitergehende Überwachungspflichten aufzuerlegen. Diese Kompetenz ist mit diesem Artikel umgesetzt.

Die Bestimmung ist gleich aufgebaut wie Artikel 21, der die Voraussetzungen für weitergehende Auskunftspflichten für Anbieterinnen abgeleiteter Kommunikationsdienste regelt. Einziger Unterschied zu Artikel 21 bildet die alternativ zu erfüllende Voraussetzung von zehn Überwachungsaufträgen. Ansonsten ist der Regelungsgegenstand beider Bestimmungen gleich, weshalb für die weiteren Ausführungen auf die Erläuterungen beim Artikel 21 verwiesen werden kann.

Bei den zu erfüllenden Pflichten handelt es sich um dieselben Pflichten, die von den Fernmeldedienstanbieterinnen zu erfüllen sind, das heisst insbesondere die

Pflichten nach Artikel 26 Absatz 1 und 3-5 BÜPF. Sie müssen also insbesondere aktive Vorbereitungen treffen, um die standardisierten Überwachungstypen nach dem 3. Kapitel Abschnitt 7 bis 12 selbst auszuführen oder durch Dritte ausführen zu lassen und die Randdaten des Fernmeldeverkehrs während 6 Monaten aufzubewahren. Die für die Anbieterinnen von Fernmeldediensten geltenden Bestimmungen des BÜPF sind sinngemäss auf die Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten anwendbar (Art. 27 Abs. 3 BÜPF).

Art. 51 Zugang zu den Anlagen

Bei Mitwirkungspflichtigen, die Überwachungsaufträge aufgrund der gesetzlichen Vorgaben nicht aktiv auszuführen haben (so bspw. FDA mit reduzierten Überwachungspflichten nach Art. 49) oder solche, die aufgrund mangelnder oder fehlender Überwachungsbereitschaft nicht in der Lage sind, einen Überwachungsauftrag auszuführen, führt der Dienst ÜPF den Überwachungsauftrag entweder selbst aus oder lässt diesen durch einen Dritten ausführen (Art. 26 Abs. 2 und 6 sowie Art. 34 BÜPF). Um einen solchen Überwachungsauftrag auszuführen, muss der Dienst ÜPF beziehungsweise die von ihm beauftragten Dritten Zugang zu den Anlagen der betreffenden Mitwirkungspflichtigen haben.

Dieser Artikel führt näher aus, was unter der Gewährung des Zugangs zu den Anlagen einer Mitwirkungspflichtigen zu verstehen ist. Zugang zu den Anlagen bedeutet demnach insbesondere Zugang zu Gebäuden, Infrastrukturen, Geräten, Leitungen, Systemen, Netzen und Diensten (Abs. 1). Die Mitwirkungspflichtige muss dem Dienst ÜPF oder den von ihm beauftragten Dritten auch ihre bestehenden Netzzugänge zu öffentlichen Fernmeldenetzen (z. B. Internetanschluss) zur Verfügung stellen (Abs. 2). Hierfür kann die Mitwirkungspflichtige dem Dienst ÜPF keine Kosten in Rechnung stellen, sondern sie hat den Netzzugang kostenlos zur Verfügung zu stellen. Sind für die Ausführung eines Überwachungsauftrages Netzzugänge zu öffentlichen Fernmeldenetzen notwendig und verfügt die Mitwirkungspflichtige nicht über solche, hat sie solche zu erstellen, soweit dies ihr zugemutet werden kann.

8. Abschnitt: Typen der Echtzeitüberwachung von Netzzugangsdiensten

Art. 52 Überwachungstyp RT_15_NA_IRI: Echtzeitüberwachung von Randdaten bei Netzzugangsdiensten

Die Bestimmung definiert den standardisierten Überwachungstyp Echtzeitüberwachung eines Netzzugangsdienstes (entspricht dem bisherigen Überwachungstyp PS 2). Im Gegensatz zum Artikel 53 sind im Rahmen eines Überwachungsauftrages nach Artikel 52 lediglich die Randdaten des Fernmeldeverkehrs auszuleiten. Dieser Überwachungstyp kommt vorrangig bei mobilen Internetzugängen zum Einsatz, um die Standortinformationen in Echtzeit zu erhalten.

Im Rahmen dieses Überwachungstyps werden generell keine Randdaten von Anwendungen erfasst. Wenn beispielsweise über den überwachten Netzzugang eine Anwendung wie VoIP benutzt wird, werden die Randdaten der Anwendung mit dem hier definierten Überwachungstyp nicht ausgeleitet. Für die Überwachung der Anwendung ist ein entsprechender Überwachungstyp vorgesehen. Als weiteres Beispiel können die MMS-Mitteilungen aufgeführt werden. So werden im Rahmen des Überwachungstyps RT_15_NA_IRI nach Artikel 52 die MMS-spezifischen Randdaten (MMS ist eine Anwendung) nicht ausgeleitet, sondern nur die Randdaten des Netzzugangs. Die MMS-spezifischen Randdaten und die Inhaltsdaten von MMS-Mitteilungen sind jedoch im Rahmen des Überwachungstyps RT_16_NA_CC_IRI nach Artikel 53 in den Inhaltsdaten verfügbar.

Absatz 1 hält fest, welche Randdaten des Fernmeldeverkehrs, der über den überwachten Netzzugangsdienstes gesendet oder empfangen wird, in Echtzeit zu übermitteln sind. Zu den in *Absatz 1 Buchstabe e* genannten Adressierungselementen des Netzzugangsdienstes gehört beispielsweise, sofern vorhanden, die Telefonnummer des zu einem DSL-Anschluss zugehörigen Telefonanschlusses. Mit den in *Absatz 1 Buchstabe g* aufgeführten "technischen Änderungen" sind Ereignisse gemeint, welche die technischen Eigenschaften des überwachten Netzzugangs verändern oder die dessen Mobility Management betreffen, so zum Beispiel Bearer Modification oder Location Update. Der Begriff "Üblicher technischer Betrieb" (*Abs. 1 Bst. h*) bedeutet, dass sich der technische Betrieb (z.B. Signalisierung, Routing) für den überwachten Teilnehmenden (Target) grundsätzlich nicht von einem nicht-überwachten Teilnehmenden unterscheidet.

Absatz 2 regelt näher, was die Standortangaben nach Absatz 1 Buchstabe h umfassen. Die Mitwirkungspflichtige hat dabei für die Übermittlung der Standortangaben die Wahl zwischen drei verschiedenen Varianten. Sie darf aber nur verifizierte, das heisst vom Netzwerk bestimmte Standortangaben liefern, da Standortangaben, die vom Endgerät oder von einer Applikation stammen, verfälscht sein könnten.

Gemäss *Buchstabe a* hat die Mitwirkungspflichtige unter anderem, die Hauptstrahlungsrichtung der Zelle mitzuteilen. Die Hauptstrahlungsrichtung ist jedoch nur mitzuteilen, wenn sie vorhanden und korrekt ist. So darf beispielsweise bei Antennen mit mehreren Sektoren nicht ein Mittelwert für die Hauptstrahlungsrichtung gebildet werden, sondern es müssen die Hauptstrahlungsrichtungen jedes Sektors mitgeteilt werden. Bei einer einfachen Zelle beschreibt die Hauptstrahlungsrichtung der Antenne der Zelle den Winkel in Grad [°] zwischen geografisch-Nord und dem Hauptstrahl. Bei einer komplexen Zelle kann dieses Datenfeld mehrere verschiedene Hauptstrahlungsrichtungen enthalten. Bei einer omnidirektionalen Zelle (gleichmässige Abstrahlung in alle Richtungen) ist dieses Datenfeld hingegen leer.

Buchstabe c stellt eine alternative Möglichkeit zu *Buchstabe a* und *b* dar. Die Bestimmung verweist lediglich auf die bisher geltenden und zukünftigen internationalen Standards, welche die Mitteilung der Standortangaben betreffen. Dadurch soll verhindert werden, dass die Verordnung jedes Mal angepasst werden muss, wenn die entsprechenden internationalen Standards angepasst beziehungsweise solche neu erlassen werden.

Art. 53 Überwachungstyp RT_16_NA_CC_IRI: Echtzeitüberwachung von Inhalten und Randdaten bei Netzzugangsdiensten

Der in *Artikel 53* definierte Überwachungstyp entspricht dem bisherigen Typ PS 1. Im Rahmen dieses Überwachungstyps hat die Mitwirkungspflichtige den gesamten Fernmeldeverkehr, der über den überwachten Netzzugang, beispielsweise mobiler Internetzugang gesendet (upload) oder empfangen (download) wird, das heisst, die Inhaltsdaten (Communication Content) sowie die zugehörigen Randdaten (IRI), die in Artikel 52 aufgeführt sind, in Echtzeit auszuleiten.

Wie bei Artikel 48 Absatz 4 erläutert, muss die Mitwirkungspflichtige grundsätzlich sicherstellen, dass jeglicher über die von ihr kontrollierte Infrastruktur geführter Fernmeldeverkehr überwacht werden kann. Ausgeleitet werden muss aber nur derjenige Fernmeldeverkehr, der an den überwachten Netzzugang gerichtet ist, beziehungsweise von diesem stammt. Bei der Benutzung fremder inländischer Infrastruktur, zum Beispiel nationales Roaming, Mobile Virtual Network Operator (MVNO), hat die Mitwirkungspflichtige sicherzustellen, dass der gesamte zu überwachende Fernmeldeverkehr von ihr oder von Dritten ausgeleitet wird.

Bei der Benutzung ausländischer Infrastruktur (z.B. Roaming im Ausland) ist der Fernmeldeverkehr nur insoweit zu überwachen, wie er von der Mitwirkungspflichtigen kontrolliert werden kann. Kontrolliert die Mitwirkungspflichtige jedoch die ausländische Infrastruktur, muss sie die zu überwachenden Kommunikationsinhalte und Randdaten vollständig ausleiten.

Eine Besonderheit stellen die mit einem Mobiltelefoniedienst assoziierten MMS-Dienste dar, da die Inhaltsdaten von MMS nicht als Anwendung (siehe 9. Abschnitt) sondern am Netzzugang im Rahmen des hier definierten Überwachungstyps mitüberwacht werden. Gemäss den ETSI-Standards werden Inhaltsdaten von eingehenden und ausgehenden MMS-Mitteilungen als Teil des Datenstroms bei der Zugangsüberwachung ausgeleitet, das heisst die MMS-Überwachung ist automatisch bei der Zugangsüberwachung eines mobilen Internetzugangs inklusive. Allerdings werden für MMS-Mitteilungen bei der Echtzeitüberwachung des Netzzugangs keine MMS-spezifischen Randdaten ausgeleitet.

Je nach Art des Netzzugangs (fix oder mobile) beziehungsweise Technologie liegen diesem Überwachungstyp die folgenden ETSI-Standards zugrunde:

- mobiler Netzzugang (GPRS, UMTS, EPS (LTE), WLAN-Interworking): ETSI TS 101 671, TS 133 108, TS 102 232-1, TS 102 232-7,
- fixer Netzzugang: ETSI TS TS 102 232-1, TS 102 232-3,
- TS 102 232-7.

9. Abschnitt: Typen der Echtzeitüberwachung von Anwendungen

Art. 54 Überwachungstyp RT_17_TEL_IRI: Echtzeitüberwachung von Randdaten bei Telefonie- und Multimediadiensten

Die Bestimmung definiert den standardisierten Überwachungstyp Echtzeitüberwachung von Telefonie- und Multimediadiensten (entspricht dem bisherigen Überwachungstyp CS 2 und CS 3), weshalb auf die Erläuterungen beim Artikel 55 verwiesen werden kann. Im Gegensatz zum Artikel 55 sind im Rahmen eines Überwachungsauftrages nach Artikel 54 lediglich die Randdaten des Fernmeldeverkehrs in Echtzeit auszuleiten, zu denen auch die Standortangaben gehören. Die einzige Ausnahme bilden die Inhaltsdaten von SMS, welche aus technischen Gründen in den Randdaten in Echtzeit enthalten sein können und deshalb zusammen mit diesen ausgeleitet werden.

Absatz 1 hält fest, welche Randdaten in Echtzeit zu übermitteln sind. Die in *Buchstabe b* bezeichneten Informationen über Registrierungsereignisse und die entsprechenden Antworten beziehen sich zum Beispiel auf die SIP-Anfragemethode "REGISTER" (siehe RFC 3261). Entsprechend ist unter Subskriptionsereignis zum Beispiel die SIP-Anfragemethode "SUBSCRIBE" (siehe RFC 6665) zu verstehen. Mit den in *Buchstabe e* aufgeführten "technischen Änderungen" sind Ereignisse gemeint, die die technischen Eigenschaften des überwachten Dienstes verändern oder die dessen Mobility Management betreffen, so zum Beispiel Bearer Modification oder Location Update. Bei ortsunabhängigen Diensten sind die im Rahmen des üblichen technischen Betriebs verfügbaren momentanen Standortangaben zu liefern (Bst. e Ziff. 9), die in Absatz 2 näher beschrieben sind. Für Ausführungen zu den Standortangaben siehe die Erläuterungen zu Artikel 52 Absatz 2.

Für ausgehende Verbindungen und Verbindungsversuche, die mit Hilfe der freien Wahl der Dienstanbieterin (Carrier Selection) hergestellt werden, hat die Anbieterin des Telefoniedienstes ebenfalls die Randdaten zu liefern.

Art. 55 Überwachungstyp RT_18_TEL_CC_IRI: - Echtzeitüberwachung von Inhalten und Randdaten bei Telefonie- und Multimediadiensten

Der in diesem Artikel definierte Überwachungstyp basiert auf den bisherigen Typen CS1, CS2 und CS3. Die Überwachung der klassischen leitungsvermittelten Telefoniedienste wird jedoch auf paketvermittelte Telefoniedienste und Multimediadienste ausgeweitet. Zu den Telefonie- und Multimediadiensten gehören auch die mit diesen konvergierenden Dienste, so insbesondere SMS, Voice Mail und RCS (bezüglich der Begriffe und Abkürzungen siehe Anhang 1). Unter *konvergierenden Diensten* sind alle Anwendungen zu verstehen, welche die Mitwirkungspflichtige dem Teilnehmenden in engem Zusammenhang mit dem Telefonie- und Multimediadienst beziehungsweise als Teil von diesem erbringt, so beispielsweise Mobiltelefonie mit SMS, VoiceMail und RCS oder Festnetztelefonie konvergierend mit Mobiltelefonie. Sogenannte Multiple-Play-Produkte, bei denen verschiedene Dienste wie Telefonie, Internetzugang und TV in einem Paket vermarktet werden, gehören jedoch nicht zu den konvergierenden Diensten.

Ein bekanntes Beispiel für paketvermittelte Telefoniedienste ist Voice over IP (VoIP), auch Internet-Telefonie genannt. Im Bereich Mobiltelefonie sind in erster

Linie VoLTE (Voice over LTE, d.h. Mobiltelefonie in 4G-Netzen) und VoWLAN (Mobiltelefonie über Wireless LAN, sog. non-3GPP Access) zu nennen. Im Bereich Multimediadienste gibt es beispielsweise ViLTE (Video over LTE, d.h. Videotelefonie in 4G-Netzen).

Die Telefonie- und Multimediadienste werden in der Regel als Anwendung überwacht und nicht am Netzzugang. Zwar sind bei Mobiltelefonie und leitungsgebundener Telefonie die Anbieterinnen des Zugangs (z.B. Telefonanschluss oder Mobilfunkzugang) und der Anwendung (Telefoniedienst) oft noch identisch, jedoch ist diese Kopplung bei modernen Diensten wie VoIP nicht mehr unbedingt gegeben. Auch in den klassischen Telefonnetzen schreitet die Entbündelung der Anschlüsse voran und es gibt die freie Wahl der Dienstanbieterin (Carrier Selection; Art. 9 der Verordnung der Eidgenössischen Kommunikationskommission vom 17. November 1997[43] betreffend das Fernmeldegesetz). Im Mobilfunkbereich sind bei einem Mobile Virtual Network Operator (MVNO) und beim Roaming die Anbieterin des Funkzugangsnetzes (Radio Access Network) und die Dienstanbieterin nicht identisch. Im IP Multimedia Subsystem (IMS) kann der Netzzugang auch über Netze anderer Anbieterinnen erfolgen, die keine Mobilfunknetze sind (sog. non-3GPP Access). Dies sind nur einige Beispiele, bei denen die Netzzugangsanbieterin nicht identisch ist mit der Dienstanbieterin des Teilnehmenden.

Im Rahmen dieses Überwachungstyps hat die Mitwirkungspflichtige den gesamten Fernmeldeverkehr, der über den überwachten Telefonie- und Multimediadienst und die mit diesem konvergierenden Dienste abgewickelt wird, das heisst die Inhaltsdaten (Communication Content) sowie die zugehörigen Randdaten (IRI), die in Artikel 54 aufgeführt sind, in Echtzeit auszuleiten.

Für ausgehende Verbindungen und Verbindungsversuche, die mit Hilfe der freien Wahl der Dienstanbieterin (Carrier Selection) hergestellt werden, hat die Anbieterin des Telefoniedienstes ebenfalls die Inhalts- und Randdaten zu liefern.

Art. 56 Überwachungstyp RT_19_EMAIL_IRI: Echtzeitüberwachung von Randdaten bei E-Mail-Diensten

Die Bestimmung definiert analog zu Artikel 57 den standardisierten Überwachungstyp Echtzeitüberwachung von E-Mail-Diensten (entspricht dem bisherigen Überwachungstyp PS 4). Nach bisherigem Recht war eine E-Mail-Anbieterin jedoch nur dann verpflichtet, eine E-Mail-Überwachung auszuführen, wenn sie zugleich auch Internetzugangsanbieterin war (Art. 15 Abs. 4 BÜPF vom 6.10.2000)[44]. Neu entfällt diese Einschränkung. Die Überwachung und Ausleitung erfolgt technisch nur noch nach dem ETSI-Standard TS 102 232-2. Die frühere Schweizer proprietäre Lösung wird nur noch während einer Übergangszeit (siehe Art. 73) unterstützt.

Im Gegensatz zum Artikel 57 sind im Rahmen eines Überwachungsauftrages nach Artikel 56 lediglich die Randdaten des überwachten E-Mail-Kontos in Echtzeit auszuleiten. Dazu gehören die SMTP-Envelop-Informationen. Im Rahmen dieses Überwachungstyps dürfen keine Inhaltsdaten ausgeleitet werden, also beispielsweise nicht der E-Mail-Header mit dem Betreff (subject).

43 SR **784.101.112**
44 Siehe auch BBl **1998** 4279 ad Art. 13 Abs. 3.

Es sind sowohl die Mail-Server-Operationen, wie Mail Send, Mail Receive, Speichern der E-Mail im Message Store (Mailbox), als auch die Zugriffe von Mail Clients auf den Mail Server zu überwachen, d.h. Operationen wie das Anmelden und Abmelden des Benutzers an der Mailbox bzw. entsprechende Versuche (*Bst. a*), das Herunterladen einer E-Mail von der Mailbox oder das Löschen einer E-Mail. Die wichtigsten Parameter der Randdaten sind in den Buchstaben a–d aufgeführt. Dazu gehören auch die AAA-Informationen ohne Passwort (*Bst. b*). Die Ereignisse, für die ein IRI zu generieren ist, sind in *Buchstabe d* summarisch dargestellt. Die Einzelheiten sind im ETSI-Standard TS 102 232-2 und im Anhang 1 der VD-ÜPF definiert. Zu beachten ist, dass auch interne E-Mails, d.h. Mailboxen, die vom gleichen Mail Server bedient werden, zu überwachen sind und dass auch die zum überwachten E-Mail-Konto zugehörigen Alias-Adressen und Verteilerlisten mit überwacht werden (zu den Begriffen Alias-Adresse und Mailingliste siehe die Erläuterungen zu Art. 40).

Art. 57 Überwachungstyp RT_20_EMAIL_CC_IRI: Echtzeitüberwachung von Inhalten und Randdaten bei E-Mail-Diensten

Der in diesem Artikel definierte Überwachungstyp basiert auf dem bisherigen Typ PS3. Es sind sowohl die Inhalts- als auch die Randdaten des überwachten E-Mail-Kontos in Echtzeit auszuleiten (siehe die Erläuterungen zu Art. 56). Die Anbieterin hat von ihr angebrachte Verschlüsselungen zu entfernen (Art. 26 Abs. 2 Bst. c BÜPF).

Art. 58 Überwachungstyp RT_21_COM_IRI: Echtzeitüberwachung von Randdaten bei anderen Fernmeldediensten oder abgeleiteten Kommunikationsdiensten

Der in *Artikel 58* definierte Überwachungstyp basiert im Prinzip auf dem bisherigen Typ PS4 (Echtzeitüberwachung der Randdaten einer Anwendung). Gemeint ist hier vor allem die Überwachung von sogenannten "Over the Top Diensten" (OTT), deren Begriffsdefinition jedoch nicht hinreichend präzise ist, um diese Dienstkategorie sauber von denen der anderen Überwachungstypen abgrenzen zu können.

Beispielsweise fallen Kommunikationsdienste in der Cloud, über Proxies oder in Sozialen Netzen in diese Kategorie. Zu beachten ist, dass für diesen Überwachungstyp derzeit noch keine spezifischen internationalen Standards existieren. Angeordnete Überwachungsmassnahmen dieses Typs werden daher vorläufig als besondere Überwachungsmassnahmen (sog. Spezialfälle) vom Dienst ÜPF ausgeführt und so in Rechnung gestellt. Der Dienst ÜPF wird die weitere Entwicklung der internationalen Standardisierung beobachten und nach der Veröffentlichung allfälliger neuer Standards die Ausführungsverordnungen zum BÜPF zeitgerecht ergänzen.

Im Unterschied zum Überwachungstyp RT_22_COM_CC_IRI (Art. 59) werden bei diesem Überwachungstyp nur die Randdaten des Fernmeldeverkehrs durch die Dienstanbieterin in Echtzeit ausgeleitet, aber keine Inhaltsdaten (siehe auch Ende der Erläuterungen zu Art. 59). Unter den *Buchstaben a-e* werden die zu liefernden Randdaten grob bestimmt.

Art. 59 Überwachungstyp RT_22_COM_CC_IRI: Echtzeitüberwachung von Inhalten und Randdaten bei anderen Fernmeldediensten oder abgeleiteten Kommunikationsdiensten

Dieser Überwachungstyp basiert im Prinzip auf dem bisherigen Typ PS3 (Echtzeitüberwachung einer Anwendung). Die Inhalts- und Randdaten können vorläufig am Netzzugang oder wie Telefonie- und Multimediadienste überwacht und ausgeleitet werden (siehe Erläuterungen zu Art. 58).

10. Abschnitt: Typen der rückwirkenden Überwachung

Die zum Zwecke der rückwirkenden Überwachung (Art. 26 Abs. 4 BÜPF) und der Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF) gesammelten Randdaten werden in der Fachsprache als «aufbewahrte Daten» («retained data») bezeichnet. Umgangssprachlich werden auch die Begriffe Vorratsdaten und Vorratsdatenspeicherung verwendet, da die Randdaten aller Teilnehmenden sozusagen auf Vorrat gespeichert werden. Im BÜPF wird die Formulierung *aufbewahrte Randdaten des vergangenen Fernmeldeverkehrs* (Art. 26 Abs. 4 BÜPF) verwendet. Da die Überwachung des vergangenen Fernmeldeverkehrs als *rückwirkende Überwachung* bezeichnet wird, gibt es auch noch die alternative Formulierung *Randdaten des vergangenen Fernmeldeverkehrs*. Im 3. Kapitel, das ausschliesslich dem Fernmeldeverkehr gewidmet ist, wird in den Erläuterungen eher die Kurzform *aufbewahrte Randdaten* verwendet.

Gestützt auf die Kompetenz, die dem Bundesrat in Artikel 31 BÜPF übertragen wird, werden im *10. Abschnitt* die Randdaten bestimmt, welche zum Zwecke der rückwirkenden Überwachung aufzubewahren und zu liefern sind.

Die zum Zwecke der Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF) aufzubewahrenden Randdaten werden im 4. und 5. Abschnitt des 3. Kapitels bestimmt.

Die aufbewahrten Randdaten des vergangenen Fernmeldeverkehrs, das heisst die Randdaten, die bei einer rückwirkenden Überwachung beschafft werden, sind nicht identisch mit den Randdaten in Echtzeit (IRI), die bei einer Echtzeitüberwachung ausgeleitet werden. Beispielsweise liefert eine Echtzeitüberwachung auch Randdaten zu Ereignissen, die nicht im Zusammenhang mit Kommunikationen oder Kommunikationsversuchen stehen (z.B. Location Update). Andererseits gibt es auch Anwendungen (z.B. MMS), für die spezifische *aufbewahrte Randdaten* standardisiert sind, aber keine spezifischen Echtzeit-Randdaten (IRI).

Gemäss den Erläuterungen in der Botschaft zum BÜPF vom 27. Februar 2013 betreffend Artikel 26 Absatz 1 Buchstabe b BÜPF[45] müssen nunmehr nicht nur die Randdaten von erfolgreichen Kommunikationen, Anmeldungen (Login) beziehungsweise Herstellungen des Netzzugangs, sondern auch jene von entsprechenden Versuchen aufbewahrt werden.

Bei Telefonie- und Multimediadiensten gilt in diesem Sinne als Kommunikationsversuch, wenn die Verbindung erfolgreich aufgebaut wurde, der Anruf aber unbeantwortet bleibt oder das Netzwerkmanagement eingegriffen hat.

45 BBl **2013** 2739.

Im Folgenden seien zwei Beispiele für Kommunikationsversuche genannt: 1. Der Anrufer wählt eine gültige Nummer, lässt es kurz klingeln und legt sofort wieder auf; 2. Der Anrufer wählt eine gültige Nummer und erhält die Ansage, dass der angerufene Teilnehmer momentan nicht erreichbar ist. Wenn der Anrufer im zweiten Beispiel dagegen auf eine VoiceMail weitergeleitet wird, stellt dies bereits eine Kommunikation dar. Ein Gegenbeispiel in diesem Sinne, welches weder eine Kommunikation, noch einen Kommunikationsversuch darstellt, ist die Wahl einer unvollständigen oder nicht-existenten Nummer.

Bei den E-Mail-Diensten und Mitteilungsdiensten gibt es in diesem Sinne keine Kommunikationsversuche, da bereits eine erfolgreiche Übermittlung der E-Mail beziehungsweise Mitteilung an den Mailserver beziehungsweise Messaging Server als Kommunikation gilt, selbst wenn die Übermittlung der E-Mail beziehungsweise Mitteilung an den Empfänger danach scheitern sollte. Dementsprechend gibt es auch bei den anderen Fernmelde- und abgeleiteten Kommunikationsdiensten keine Kommunikationsversuche.

Als Anmeldeversuch beziehungsweise versuchte Herstellung des Netzzugangs gilt in diesem Sinne, wenn die Authentifizierung des Teilnehmenden erfolgreich war, aber die Anmeldung beziehungsweise der Netzzugang aus anderen Gründen nicht zustande kam, beispielsweise wegen mangelndem Guthaben.

Die Randdaten von solchen Versuchen müssen jedoch nur nach Massgabe des Artikels 48 Absatz 4 von der Mitwirkungspflichtigen aufbewahrt werden. Wenn beispielsweise Anrufversuche von anderen Netzen abgebrochen werden, bevor die Signalisierung das Netz der Mitwirkungspflichtigen erreicht (in diesem Fall klingelt das angerufene Telefon nicht), kann die Mitwirkungspflichtige die Randdaten solcher Kommunikationsversuche nicht aufbewahren, da sie sie nicht besitzt.

Weiterhin kann es vorkommen, dass Kommunikationen und Kommunikationsversuche nur unvollständige Adressierungselemente enthalten oder manche Adressierungselemente fehlen. Beispielsweise könnte bei Anrufen aus dem Ausland die Nummer des Anrufenden unvollständig sein oder sogar fehlen. Die entsprechend aufbewahrten Randdaten würden dann bei einer rückwirkenden Überwachung dieser ausländischen Nummer (Zielidentifikator) nicht gefunden werden können, da in diesem Beispiel der Zielidentifikator in den entsprechenden aufbewahrten Randdaten unvollständig beziehungsweise nicht vorhanden wäre.

Für alle Typen der rückwirkenden Überwachung (Art. 60-66) gilt, dass die dort beschriebenen *aufbewahrten Randdaten* auf dem ETSI-Standard TS 102 657 basieren.

Art. 60 Überwachungstyp HD_23_NA: rückwirkende Überwachung von Randdaten bei Netzzugangsdiensten

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Überwachungstyp PS5 und dient zur rückwirkenden Überwachung eines Internetzugangs. Dabei werden die aufbewahrten Randdaten des vergangenen Fernmeldeverkehrs übermittelt, der über den überwachten Netzzugangsdienst gesendet oder empfangen wurde. Die Randdaten sind auch bei Netzzugangsversuchen aufzubewahren. Was unter einem Netzzugangsversuch zu verstehen ist, wurde einleitend zum 10. Abschnitt erläutert (siehe oben).

Die *Buchstaben a–g* halten fest, welche Daten die betreffenden Mitwirkungspflichtigen zu speichern und zu liefern haben. Es handelt sich um folgende Daten: das Datum und die Uhrzeit, wann der Netzzugang hergestellt beziehungsweise dies versucht wurde und wann er getrennt wurde (*Bst. a*), die Art des Netzzugangs (*Bst. b*), die verwendeten Authentifizierungs-, Autorisierungs- und Abrechnungsdaten (*Bst. c*), die durch die Netzzugangsanbieterin zugeteilten IP-Adressen beziehungsweise Adressbereiche und das Datum und die Uhrzeit der jeweiligen Zuteilung (*Bst. d*) und die Adressierungselemente des Netzzugangsdienstes (*Bst. e*), zu denen beispielsweise, die Telefonnummer des zu einem DSL-Anschluss zugehörigen Telefonanschlusses oder die MSISDN eines mobilen Netzzugangs gehört. Weiterhin gehören zu diesen Daten die Geräteidentifikatoren der Endgeräte (*Bst. f*) und, sofern verfügbar, die jeweiligen Datenmengen, welche innerhalb der Sitzung hochgeladen und heruntergeladen wurden (*Bst. g*). Bei ortsunabhängigen Diensten sind zusätzlich zu den in den Buchstaben a–g erwähnten Daten die im Rahmen des üblichen technischen Betriebes verfügbaren Standortangaben zu Beginn und, falls zutreffend am Ende der Sitzung zu übermitteln (*Bst. h*). Die Bedeutung der Formulierung "üblicher technischer Betrieb", wird bei Artikel 52 Absatz 1 Buchstabe h erläutert. Die Mitwirkungspflichtige hat bei der Übermittlung der Standortangaben nach Buchstabe h die Wahl zwischen drei verschiedenen Varianten. Sie darf aber nur verifizierte, das heisst vom Netzwerk bestimmte Standortangaben liefern. Nicht akzeptiert werden Standortangaben, die vom Endgerät oder von einer Applikation stammen, da solche verfälscht sein können.

Art. 61 Überwachungstyp HD_24_TEL: rückwirkende Überwachung von Randdaten bei Telefonie- und Multimediadiensten

Der in diesem Artikel definierte Überwachungstyp basiert auf dem bisherigen Typ CS4 (rückwirkende Überwachung eines Telefoniedienstes) und wurde um die Multimediadienste erweitert. Er dient zur rückwirkenden Überwachung von Telefonie- und Multimediadiensten, das heisst zur Beschaffung der aufbewahrten Randdaten dieser Dienste. Die Begriffe *Telefonie- und Multimediadienste* und *konvergierende Dienste* werden bei Artikel 55 erläutert.

Für ausgehende Verbindungen und Verbindungsversuche, die mit Hilfe der in den Erläuterungen zu Artikel 55 beschriebenen freien Wahl der Dienstanbieterin (Carrier Selection) hergestellt wurden, hat die Anbieterin des Telefoniedienstes ebenfalls die Randdaten zu liefern. Die Mitwirkungspflichtige muss in der Lage sein, bei der rückwirkenden Überwachung die Übereinstimmung von E.164-Nummern zu erkennen, auch wenn sie in verschiedenen Formaten (national, international) vorliegen.

Im Gegensatz zur Echtzeitüberwachung, bei der die MMS-Dienste am Netzzugang mitüberwacht werden, überwacht man sie rückwirkend als Anwendung, jedoch nicht als eigenständige Überwachung, sondern im Rahmen des hier definierten Überwachungstyps.

Die *Buchstaben a–d* halten fest, welche Daten die betreffenden Mitwirkungspflichtigen zu speichern und zu liefern haben. Was unter einem *Kommunikationsversuch* (*Bst. b*) zu verstehen ist, wurde einleitend zum 10. Abschnitt erläutert (siehe oben). Zu den in *Buchstabe b Ziffer 5* bezeichneten verfügbaren Adressen gehört im Falle von VoIP auch die Adresse des SIP-Proxy.

Bei ortsunabhängigen Diensten gilt wie bei Artikel 60, dass die im Rahmen des üblichen technischen Betriebes verfügbaren Standortangaben zu Beginn und, falls zutreffend, am Ende der Kommunikation zu übermitteln sind (*Bst. d*). Die Bedeutung der Formulierung "üblicher technischer Betrieb" wurde bei Artikel 52 Absatz 1 Buchstabe h erläutert.

Die Mitwirkungspflichtige hat bei der Übermittlung der Standortangaben gemäss *Buchstabe d Ziffer 1* die Wahl zwischen drei verschiedenen Varianten. Sie darf aber nur verifizierte, das heisst vom Netzwerk bestimmte Standortangaben liefern. Nicht akzeptiert werden Standortangaben, die vom Endgerät oder von einer Applikation stammen, da solche verfälscht sein können.

Bei anderen ortsunabhängigen Diensten (*Bst. d Ziff. 2*), womit zum Beispiel nomadische Dienste wie VoIP gemeint sind, sind die Standortangaben des Zugangs zu den überwachten Dienstes zu speichern und zu liefern. Nomadische Dienste können praktisch an jedem Internetzugang benutzt werden und sind daher ortsunabhängig. Die Standortangaben des Zugangs zum Dienst müssen nur dann aufbewahrt und geliefert werden, wenn sie verfügbar sind.

Art. 62 Überwachungstyp HD_25_EMAIL: rückwirkende Überwachung von Randdaten bei E-Mail-Diensten

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ PS6 (rückwirkende Überwachung eines asynchronen elektronischen Postdienstes). Die *Buchstaben a* und *b* halten fest, welche Daten die betreffenden Mitwirkungspflichtigen zu speichern und zu liefern haben. Der Schwerpunkt liegt dabei auf den Ereignissen Senden und Empfangen einer Nachricht sowie An- und Abmeldevorgängen an der Mailbox. Das Ereignis des Herunterladens einer Nachricht schliesst auch teilweises Herunterladen mit ein. Die Informationen zu den weiteren Ereignissen sind nur soweit vorhanden aufzubewahren und zu liefern. Mit dieser flexiblen Regelung wird berücksichtigt, dass viele Anbieterinnen von E-Mail-Diensten bereits seit langem ihre Anlagen in Betrieb haben, die die Überwachung der Schwerpunktereignisse unterstützen. Für die Überwachung der weiteren Ereignisse müssten diese Systeme jedoch angepasst werden, was nicht verhältnismässig wäre. Bei neuen Systemen sollen jedoch alle der in den Buchstaben a und b angegebenen Daten aufbewahrt und geliefert werden.

Art. 63 Überwachungstyp HD_26_COM: rückwirkende Überwachung von Randdaten bei anderen Fernmeldediensten oder abgeleiteten Kommunikationsdiensten

Der in diesem Artikel definierte rückwirkende Überwachungstyp existierte bisher noch nicht. Der technische Fortschritt und die weitverbreitete Nutzung dieser neuen Dienste machen jedoch die Ausdehnung der rückwirkenden Überwachung auf diese Dienste erforderlich. Da für diese Dienste noch keine ETSI-Standards veröffentlicht wurden, müssen vorerst nur die vorhandenen Daten geliefert werden. Das Format der Datenlieferung orientiert sich an vergleichbaren, bereits standardisierten Fernmelde- und abgeleiteten Kommunikationsdiensten. Es sind aber auch andere Formate möglich, falls die Mitwirkungspflichtige bereits Prozesse und Systeme für diesen Zweck implementiert hat, beispielsweise wegen Vorschriften anderer Staaten.

Art. 64 Überwachungstyp AS_27_PREP_COV: Netzabdeckungsanalyse in Vorbereitung eines Antennensuchlaufs

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ CS5 (Netzanalyse in Vorbereitung eines Antennensuchlaufes).

Um einen Antennensuchlauf vorzubereiten, kann die anordnende Behörde beim Dienst ÜPF eine Auflistung der Mobilfunkzellen oder WLAN-Zugangspunkte (WLAN access points) verlangen, die eine gewisse geografische Position zu einer bestimmten Zeit am wahrscheinlichsten abdeckten (*Abs. 1*). Die geografische Position ist entweder mittels Koordinaten oder mittels Postadresse (siehe Erläuterungen zu Art. 67 Bst. a Ziff. 1) zu bezeichnen. Weitere Angaben wie beispielsweise Tageszeit können zu einer genaueren Bestimmung der geografischen Position beitragen. Es ist jedoch nicht zwingend, weitere Angaben zu machen.

Absatz 2 beschreibt, welche Auskunft die FDA dem Dienst ÜPF aufgrund der Anfrage zusenden muss.

Art. 65 Überwachungstyp AS_28_PREP_REF: Referenzkommunikationen oder Referenznetzzugänge in Vorbereitung eines Antennensuchlaufs

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ CS7 (Netzanalyse mittels Referenzanrufen der Strafverfolgungsbehörden in Vorbereitung eines Antennensuchlaufes).

Wie Artikel 64 dient dieser Artikel dazu, einen Antennensuchlauf vorzubereiten. Im Fall dieses Artikels liefert die anordnende Behörde dem Dienst eine Liste von Referenzgesprächen, beziehungsweise von Referenzkommunikationen und Referenznetzzugängen zur weiteren Abklärung der betroffenen Mobilfunkzellen oder WLAN-Zugangspunkte (WLAN access points).

Absatz 2 legt die Angaben fest, welche die anordnende Behörde dem Dienst ÜPF für den Auftrag liefern muss. Die FDA benötigen diese Angaben um die Mobilfunkzellen beziehungsweise die WLAN-Zugangspunkte bestimmen zu können.

Absatz 3 regelt, wie die FDA ihre Systeme aufgrund der in Absatz 2 genannten Suchkriterien durchsuchen müssen und beschreibt die Auskunft, welche die FDA dem Dienst ÜPF erteilen.

Art. 66 Überwachungstyp AS_29: Antennensuchlauf

Der in diesem Artikel definierte Überwachungstyp entspricht dem bisherigen Typ CS6 (Antennensuchlauf).

Artikel 66 regelt, welche Angaben durch die FDA zu liefern sind.

Absatz 1 definiert dabei den Umfang der Überwachung und limitiert die Überwachung auf einen Zeitraum von zwei Stunden pro Anordnung. Diese maximale Zeitspanne entspricht der bisherigen Praxis und wurde deshalb festgelegt, um den damit verbundenen Aufwand zu minimieren, die grossen Datenmengen zeitlich einzugrenzen und dem Verhältnismässigkeitsgrundsatz Rechnung zu tragen. Falls ein längerer Zeitraum für die Strafverfolgungsbehörden von Interesse ist, ist dieser längere Zeitraum in mehrere Anordnungen zu je zwei

Stunden aufzuteilen. Die Gebühren werden dabei pro Anordnung für die Dauer von zwei Stunden und pro Zelle berechnet. Das Zwangsmassnahmengericht hat jede Anordnung zu genehmigen. So soll zum Beispiel für die Zellen A, B und C bei der FDA Y für einen Zeitraum von 5 Stunden ein Antennensuchlauf durchgeführt werden. Die Strafverfolgungsbehörden ordnen den Antennensuchlauf mittels insgesamt 9 Anordnungen gegenüber dem Dienst ÜPF wie folgt an: Anordnung 1 und 2 für Zelle A für jeweils 2 Stunden und Anordnung 3 für Zelle A für 1 Stunde, analog Anordnungen 4, 5 und 6 für Zelle B und Anordnungen 7, 8 und 9 für Zelle C. Daraus resultieren Gebühren von neunmal den Gebührenansatz für einen Antennensuchlauf gemäss GebV-ÜPF.

Absatz 2 regelt, dass die Überwachungsdaten nach Absatz 1 in der für die Artikel 60 und 61 festgelegten Weise zu übermitteln sind, weshalb auf die dortigen Erläuterungen verwiesen werden kann.

11. Abschnitt: Notsuche und Fahndung

Das Gesetz ermöglicht neu die Überwachung des Postverkehrs ausserhalb von Strafverfahren im Rahmen einer Notsuche (Art. 35 Abs. 1 BÜPF) oder Fahndung (Art. 36 Abs. 1 BÜPF). Lediglich der Prozess der Anordnung und Genehmigung einer Überwachung des Postverkehrs im Rahmen einer Notsuche oder Fahndung unterscheidet sich von einer Überwachung des Postverkehrs innerhalb eines Strafverfahrens. Dafür sind aber keine eigenen Überwachungstypen oder spezielle Regelungen in der Verordnung erforderlich.

Für die Überwachung des Fernmeldeverkehrs ausserhalb von Strafverfahren im Rahmen einer Notsuche (Art. 35 BÜPF) oder Fahndung (Art. 36 BÜPF) werden spezielle Regelungen in der Verordnung getroffen. Bei den Überwachungstypen der Notsuche (Art. 67) wurden im Gegensatz zu den gewöhnlichen Überwachungstypen die Überwachung von Netzzugang und Anwendungen jeweils zusammengefasst. Dies liegt zum einen darin begründet, dass es bei Notsuchen sehr schnell gehen muss, da eine schwere Gefährdung der Gesundheit oder des Lebens der gesuchten Person besteht und der Ablauf der Anordnung durch die Strafverfolgungsbehörden an den Dienst ÜPF und die Beauftragung von diesem an die Mitwirkungspflichtigen möglichst einfach zu gestalten ist. Zum anderen sollen rasch alle verfügbaren Informationen über die Person eingeholt werden, die Ziel der Notsuche ist und deshalb muss die Mitwirkungspflichtige alle Fernmeldedienste, die sie im Zusammenhang mit den angeordneten Zielidentifikatoren erbringt, entsprechend dem angeordneten Typ der Notsuche überwachen.

An dieser Stelle ist es wichtig klarzustellen, dass gemäss Artikel 35 Absatz 3 BÜPF ebenfalls technische Geräte nach Artikel 269bis StPO (z.B. IMSI-Catcher) im Rahmen einer Notsuche eingesetzt werden können und dass es gemäss Artikel 36 Absatz 2 BÜPF ebenfalls möglich ist, technische Geräte nach Artikel 269bis StPO (z.B. IMSI-Catcher) oder besondere Informatikprogramme nach Artikel 269ter StPO (z.B. GovWare) im Rahmen einer Fahndung zu verwenden.

Art. 67 Überwachungstypen EP: Notsuche

Dieser Artikel ersetzt den Artikel 16*a* der bisherigen VÜPF, der sich auf die Suche und Rettung vermisster Personen bezieht. Das BÜPF ermöglicht neu im Rahmen der Notsuche im Bereich des Fernmeldeverkehrs die Überwachung der Kommunikationsinhalte (Bst. b). Bisher waren das sogenannte Paging (Bst. a), die Echtzeitüberwachung der Randdaten (Bst. c) und die rückwirkende Überwachung (Bst. d) möglich. Diese Typen der Notsuche werden beibehalten.

Buchstabe a beschreibt den Überwachungstyp Paging, mit dem die letzte festgestellte Aktivität (maximal 6 Monate zurück) des mobilen Endgerätes durch die Mitwirkungspflichtige in Erfahrung gebracht wird. Hierbei handelt es sich um die Standortbestimmung von mobilen Endgeräten. Die Zusammenstellung der Angaben wird in *Buchstabe a* beschrieben. Der *eindeutige Identifikator des Mobilfunknetzes* besteht aus der Mobilfunk-Landeskennzahl (Mobile Country Code, MCC) und der Mobilfunk-Netzkennzahl (Mobile Network Code, MNC). Die Ziffern 1–3 behandeln unterschiedliche Methoden der Standortbestimmung. Die Mitwirkungspflichtige muss die Standortbestimmung anhand einer der drei Ziffern durchführen und die darin beschriebenen Informationen liefern. Die in *Ziffer 1* aufgeführte *Postadresse* kann auch eine ähnliche geografische Beschreibung (z.B. Strassen-Nummer und Km-Angabe, Postleitzahl Gemeinde) des Standorts der Zelle sein, da es nicht für alle Antennenstandorte echte Postadressen gibt. Das Datenfeld *Hauptstrahlungsrichtung* kann auch leer sein oder mehrere verschiedene Hauptstrahlungsrichtungswerte und Attribute enthalten. Bei einer omnidirektionellen Zelle (gleichmässige Abstrahlung in alle Richtungen) ist dieses Datenfeld leer. Bei einer komplexen oder speziellen Zelle kann dieses Datenfeld zusätzlich zu den Hauptstrahlungsrichtungswerten beispielsweise auch folgende Attribute enthalten: inh (inhouse = Zelle innerhalb eines Gebäudes); tun (tunnel = zur Zelle gehören Repeater für die Funkabdeckung eines oder mehrerer Tunnel).

Buchstabe b beschreibt die Echtzeitüberwachung mit Inhalt und Randdaten im Rahmen einer Notsuche. Die anordnende Behörde erteilt eine Anordnung pro Mitwirkungspflichtige und pro gesuchtes Endgerät an den Dienst ÜPF, welcher dann die Notsuchen an die entsprechenden Mitwirkungspflichtigen beauftragt. Jede beauftragte Mitwirkungspflichtige richtet die jeweils zutreffenden Überwachungstypen nach den Artikeln 53 und 55 ein, so dass alle von ihr erbrachten Dienste für das gesuchte Endgerät abgedeckt sind. Damit wird der Dringlichkeit einer Notsuche Rechnung getragen, da es um die schnellstmögliche Standortbestimmung und Auffindung von Personen geht, die an Leib und Leben bedroht sind. Einzelne Aufträge pro überwachten Fernmeldedienst beziehungsweise abgeleiteten Kommunikationsdienst, wie sie sonst bei Überwachungen erteilt werden, würden bei einer Notsuche zu viel Zeit kosten. Beispiel: Die Mitwirkungspflichtige erhält einen Auftrag für die Notsuche vom Typ EP_31_RT_CC_IRI (Bst. b) für die MSISDN X. Angenommen, der Teilnehmende mit der MSISDN X hat bei der Mitwirkungspflichtigen ein Mobilabonnement mit Telefonie und Internetzugang, dann richtet die Mitwirkungspflichtige entsprechend für den Telefoniedienst eine Echtzeitüberwachung des Typs RT_18_TEL_CC_IRI und für den Netzzugang eine Echtzeitüberwachung des Typs RT_16_NA_CC_IRI ein. Die Echtzeitüberwachungen bleiben auch im Rahmen einer Notsuche so lange aktiv, bis der Dienst ÜPF die jeweiligen Aufhebungsaufträge an die entsprechenden Mitwirkungspflichtigen erteilt.

Buchstabe c beschreibt die Echtzeitüberwachung ohne Inhaltsdaten, das heisst nur der Randdaten, im Rahmen einer Notsuche. Das Vorgehen ist entsprechend wie unter Buchstabe b erläutert. Der einzige Unterschied zu Buchstabe b besteht darin, dass jede beauftragte Mitwirkungspflichtige die jeweils zutreffenden Überwachungstypen nach den Artikeln 52 und 54 einrichtet, so dass alle von ihr erbrachten Dienste für das gesuchte Endgerät abgedeckt sind.

Buchstabe d regelt die rückwirkende Notsuche beispielsweise für den Fall, dass das Endgerät nicht mehr aktiv ist. Das Vorgehen ist entsprechend wie unter Buchstabe b erläutert. Die Unterschiede zu Buchstabe b bestehen darin, dass es sich um rückwirkende Überwachungen handelt, dass jede beauftragte Mitwirkungspflichtige die jeweils zutreffenden Überwachungstypen nach den Artikeln 60 und 61 einrichtet, so dass alle von ihr erbrachten Dienste für das gesuchte Endgerät abgedeckt sind, und dass für die rückwirkenden Überwachungen keine Aufhebungsaufträge erforderlich sind.

Die Entschädigung für die Mitwirkungspflichtigen richtet sich nach der Anzahl der durch die Behörden angeordneten Notsuchen pro Mitwirkungspflichtige und pro gesuchtes Endgerät und nicht nach der Anzahl der letztlich durchgeführten Überwachungen.

Buchstabe e ermöglicht neu auch die Durchführung eines Antennensuchlaufs (Art. 66) im Rahmen einer Notsuche und diesbezügliche Vorbereitungen (Art. 64 und 65).

Art. 68 Fahndung

Dieser Artikel ist neu und regelt die Fahndung nach verurteilten Personen wie in Artikel 36 BÜPF vorgesehen. Der Typ der Fahndungsanordnung besteht aus einem Überwachungstyp der Echtzeitüberwachung "Inhalt und Randdaten" (*Bst. a*) oder aus einem Überwachungstyp der Echtzeitüberwachung "nur Randdaten" (*Bst. b*) oder aus einem Überwachungstyp der rückwirkenden Überwachung (*Bst. c*). Die Fahndungstypen entsprechen exakt den Überwachungstypen. Bei den Fahndungstypen werden also im Unterschied zu den Typen der Notsuche keine Überwachungstypen kombiniert. Zur Unterscheidung in der Statistik muss bei der Anordnung solcher Fahndungen als Grund der Überwachung das Attribut "Fahndung" angegeben werden. Falls im Rahmen einer Fahndung mehrere Überwachungstypen angeordnet werden sollen, muss pro Überwachungstyp eine Anordnung erfolgen. Bei Fahndungen gilt die übliche Gebührenregelung, dass jeder der pro Anbieterin und Zielidentifikator angeordneten Überwachungstypen gebührenpflichtig ist (siehe GebV-ÜPF).

12. Abschnitt: Netzexterne Identifikatoren

Art. 69

Artikel 69 regelt, ähnlich wie die Artikel 16*b* und 24*c* der bisherigen VÜPF, die Überwachung von netzexternen Identifikatoren. Netzexterne Identifikatoren sind Identifikatoren, die nicht von der mit der Überwachung beauftragten

Mitwirkungspflichtigen verwaltet werden oder die nicht in ihrem Netz eingebucht sind.

Hiermit wird die sogenannte Kopfschaltung geregelt. Die Kopfschaltung ist nur bei Anwendungen standardisiert, jedoch nicht beim Netzzugang. Ausserdem bestehen bei den Zielidentifikatoren Einschränkungen (z.B. keine IMSI, keine IMEI), welche im Einzelnen in der Verordnung des EJPD zur Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF) geregelt werden. Bezüglich des Begriffs Kopfschaltung wird auf die Erläuterungen in der Botschaft zum BÜPF vom 27. Februar 2013 betreffend Artikel 31 BÜPF[46] verwiesen. Im Unterschied zur bisherigen Praxis ist kein gesonderter Vermerk in der Überwachungsanordnung beziehungsweise im Überwachungsauftrag erforderlich. In Artikel 48 Absatz 4 ist allgemein geregelt, welcher Fernmeldeverkehr zu überwachen ist.

4. Kapitel: Schlussbestimmungen

Art. 70 Organisatorische, administrative und technische Vorschriften

Dieser Artikel entspricht Artikel 33 VÜPF vom 31. Oktober 2001[47] mit den nötigen Änderungen.

Artikel 70 ist, zusammen mit Artikel 31 Absatz 3 BÜPF[48], die rechtliche Grundlage für die Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF). Die Verordnung des EJPD über das Beratende Organ im Bereich der Überwachung des Post- und Fernmeldeverkehrs (Beratendes Organ) stützt sich dagegen direkt auf das BÜPF, genau auf Artikel 5 Absatz 3 BÜPF.

Gestützt auf Artikel 70 erlässt das EJPD die für die Durchführung der Überwachung des Post- und Fernmeldeverkehrs erforderlichen technischen, administrativen und organisatorischen Bestimmungen. Diese richten sich nicht nur an die Anbieterinnen von Fernmeldediensten und abgeleiteten Kommunikationsdiensten, sondern auch an die Anbieterinnen von Postdiensten.

Nach bisherigem Recht wurden die technischen und administrativen Einzelheiten durch Richtlinien des Dienstes ÜPF geregelt (Art. 33 Abs. 1bis VÜPF vom 31. Oktober 2001[49]; siehe www.li.admin.ch).

Weitere Delegationsnormen an das EJPD befinden sich in den Artikeln 31 (Abnahmeverfahren) und 47 Absatz 2 (technische Angaben in der Überwachungsanordnung) sowie im Artikel 27 Absatz 1 (Anforderungen an die Qualität der übermittelten Daten).

Der *zweite Satz* des Artikels 70 präzisiert, dass das EJPD die Fristen festsetzt, innerhalb derer die entsprechenden Daten zu liefern sind.

46 BBl **2013** 2749.
47 SR **780.11**
48 BBl **2013** 2750/2751.
49 SR **780.11**

Art. 71 Vollzug

Artikel 71 Absatz 1 entspricht im Wesentlichen dem Artikel 33 Absatz 2 VÜPF vom 31. Oktober 2001[50]. Mit dieser Regelung wird sichergestellt, dass der Dienst ÜPF weiterhin die elektronischen Formulare und Schnittstellen für alle anordnenden Behörden und Mitwirkungspflichtigen zur Verfügung stellen kann. Aus Gründen der Effizienz und Fehlervermeidung sind ausschliesslich die elektronischen Formulare und Schnittstellen des Dienstes ÜPF zu verwenden.

Absatz 2 sieht vor, dass zu einem späteren Zeitpunkt die elektronischen Formulare durch einen Online-Zugriff auf das Verarbeitungssystem des Dienstes ÜPF ersetzt werden können. Da dieser Zeitpunkt noch unbestimmt ist, kann der Dienst ÜPF selber über diese Umstellung entscheiden. Sollte der Online Zugriff auf das Verarbeitungssystem nicht möglich sein oder dieses selbst einmal ausfallen, so sollen die Formulare weiterhin zum Einsatz kommen.

Art. 72 Aufhebung und Änderung anderer Erlasse

Mit dem Inkrafttreten der vorliegenden Verordnung wird die VÜPF vom 31. Oktober 2001 aufgehoben.

Zwei andere Verordnungen werden gleichzeitig teilgeändert:

- die Organisationsverordnung vom 17. November 1999[51] für das Eidgenössische Justiz- und Polizeidepartement (OV-EJPD). Es handelt sich hier um eine formelle Anpassung des Artikels 25.

- die Verordnung vom 9. März 2007[52] über Fernmeldedienste (FDV). Es geht um Anpassungen im Artikel 3 Absatz 1 Buchstabe d und Absatz 2 sowie im Artikel 80.

Art. 73 Übergangsbestimmungen

Es ist notwendig, entsprechende Übergangsbestimmungen vorzusehen, damit die Mitwirkungspflichtigen und der Dienst ÜPF genügend Zeit für die Umsetzung der neuen Bestimmungen zur Verfügung haben. Somit kann auf ein gestaffeltes Inkrafttreten der Ausführungsverordnungen zum neuen BÜPF verzichtet werden.

Absatz 1 gibt dem Dienst ÜPF die Möglichkeit, die Statistik noch nach bisherigem Recht vorzunehmen bis die Systemkomponenten nach der Etappe 1 des Programms zum Ausbau und zum Betrieb des Verarbeitungssystems zur Fernmeldeüberwachung (V-FMÜ) sowie der polizeilichen Informationssysteme des Bundes (Programm FMÜ)[53] in Betrieb genommen wurden. Die aktuellen Systeme, vor allem das CCIS, bei welchem der Wartungsvertrag nicht mehr angepasst werden kann, ermöglichen nicht die gewünschten Statistikauszüge.

Nachdem der Dienst ÜPF die automatisierte Schnittstelle für Auskünfte in Betrieb genommen hat, haben die Mitwirkungspflichtigen nach *Absatz 2* weitere sechs Monate Zeit, um ihre Systeme entsprechend anzupassen. Anschliessend erteilen die in der Verordnung verpflichteten Mitwirkungspflichtigen ihre Auskünfte über die automatisierte Schnittstelle an den Dienst ÜPF.

50 SR **780.11**
51 SR **172.213.1**
52 SR **784.101.1**
53 BBl **2015** 3033

Nicht alle Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten gemäss Artikel 21 sind bereits heute in der Lage, die Auskünfte gemäss den neuen Auskunftstypen zu erteilen. Sie müssen entsprechende Anpassungen ihrer Software oder Systeme vornehmen. Deshalb haben sie nach *Absatz 2* zwölf Monate Zeit, um die entsprechenden Anpassungen vorzunehmen.

Den FDA und den Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten gemäss Artikel 50, die ihre Systeme anpassen müssen, damit sie auch wie neu vorgeschrieben die Randdaten zu Kommunikations- und Anmelde*versuchen* speichern und übermitteln können, wird eine Übergangsfrist von 24 Monaten gewährt (*Abs. 3*).

Die veralteten proprietären Schweizer Ausleitungsmechanismen und Prozeduren für die E-Mail-Überwachung werden in der VD-ÜPF nicht mehr unterstützt. Das Verarbeitungssystem des Dienstes ÜPF unterstützt diese noch für bereits vor Inkrafttreten dieser Verordnung operationelle Systeme während einer begrenzten Übergangszeit. Den FDA wird ein angemessener Zeitraum von 24 Monaten eingeräumt, um ihre vorhandenen Systeme zur E-Mail-Überwachung gemäss den Vorschriften dieser Verordnung und der VD-ÜPF umzustellen (*Abs. 4*).

Art. 74 Inkrafttreten

Das Inkrafttreten dieser Verordnung wurde mit dem Inkrafttreten des BÜPF und der anderen Ausführungsverordnungen koordiniert.

Auf ein gestaffeltes Inkrafttreten kann verzichtet werden.

Anhang

Tabelle Pflichten PDA/FDA

		AUSKUNFT			ÜBERWACHUNG		
		BÜPF	VÜPF	Pflichten	BÜPF	VÜPF	Pflichten
Anbieterinnen von Postdiensten (**PDA**)		_____	_____	_____	19	14	
Anbieterinnen von Fernmeldediensten (**FDA**) Art. 2 Bst. b BÜPF	KLEIN[54] (oder im Bildungs-bereich) Art. 26 Abs. 6 BÜPF	21/22	18 Abs. 1 und 3 20 29 (compliance)	A	26 Abs. 2 und 6	49	B
	NORMAL	21/22	11 Abs. 2, 18 Abs. 1 und 2, 19, 20 29 (compliance) 73 (Übergangsbest.)	C	26 Abs. 1-5	11 Abs. 2 48 29 (compliance)	D
Anbieterinnen abgeleiteter Kommunikationsdienste Art. 2 Bst. c BÜPF	NORMAL	22 Abs. 3	11 Abs. 2 18 Abs. 4	E	27 Abs. 1 und 2	11 Abs. 2	F
	GROSS[55] (weitergehende Pflichten) Art. 27 BÜPF	22 Abs. 4	18 Abs. 1 und 2 21 29 (compliance) 73 (Übergangsbest.)	G	27 Abs. 3 26 Abs. 1-5	11 Abs. 2 29 (compliance) 48 50	H

[54] Downgrade
[55] Upgrade

A. Pflichten der FDA mit reduzierten Überwachungspflichten (klein) bei Auskünften

Voraussetzung: FDA bietet Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich an.

- haben bei Auskünften die gleichen Pflichten wie "normale" FDA (kein Downgrade bei Auskünften)
- beim Pikettdienst gibt es eine Befreiung gemäss Art. 11 Abs. 2 VÜPF
- hinsichtlich der automatisierten Beantwortung von Auskunftsgesuchen nach den Artikeln 33-46 VÜPF gibt es eine Befreiung gemäss Art. 18 Abs. 3 VÜPF (sie können diese auch schriftlich beantworten)

B. Pflichten der FDA mit reduzierten Überwachungspflichten (klein) bei Überwachungen, Notsuchen und Fahndungen

Voraussetzung: FDA bietet Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich an.

- sind von den Pflichten gemäss Art. 26 Abs. 1 und 3–5 BÜPF befreit
- beim Pikettdienst gibt es eine Befreiung gemäss Art. 11 Abs. 2 VÜPF
- haben lediglich die folgenden Pflichten (gemäss Art. 26 Abs. 2 BÜPF):
  - die für die Durchführung der Überwachung notwendigen Informationen zu liefern,
  - die Überwachung zu dulden,
  - die von ihr angebrachten Verschlüsselungen zu entfernen.

C. Pflichten der FDA (normal) bei Auskünften

- liefern Auskünfte über Fernmeldedienste (Art. 21 BÜPF)
- liefern Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF)
- müssen in der Lage sein, die Auskünfte gemäss Art. 33-46 VÜPF zu beantworten (Art. 18 Abs. 1 VÜPF)
- Sofern die Abfrageschnittstelle des Verarbeitungssystems die automatische Beantwortung ausführen kann, beantworten sie die Auskunftsgesuche gemäss den Artikeln 33-40 automatisiert, jene gemäss den Artikeln 41-46 können sie auch manuell beantworten (Art. 18 Abs. 2 VÜPF).
- Aufbewahrungspflichten für die Daten gemäss Art. 21 und 22 BÜPF sowie Art. 20 VÜPF
- Art. 11 Abs. 2 VÜPF

D. Pflichten der FDA (normal) bei Überwachungen, Notsuchen und Fahndungen

- Art. 26 BÜPF (Pflichten der Anbieterinnen von Fernmeldediensten)

1 Anbieterinnen von Fernmeldediensten liefern dem Dienst oder nach Artikel 17 Buchstabe c der anordnenden Behörde oder der von dieser bezeichneten Behörde auf Verlangen:
  a. den Inhalt des Fernmeldeverkehrs der überwachten Person;
  b. die Randdaten des Fernmeldeverkehrs der überwachten Person.

2 Sie müssen zudem:
  a. die für die Durchführung der Überwachung notwendigen Informationen liefern;

b. Überwachungen dulden, die durch den Dienst oder durch von diesem beauftragte Personen durchgeführt werden; zu diesem Zweck müssen sie unverzüglich Zugang zu ihren Anlagen gewähren;
c. von ihnen angebrachte Verschlüsselungen entfernen.

3 Die Anbieterinnen von Fernmeldediensten, die an der zu überwachenden Fernmeldedienstleistung beteiligt sind, müssen ihre Daten dem Dienst oder derjenigen Anbieterin, die mit der Überwachung beauftragt ist, liefern.

4 Die Anordnung kann zur Überwachung in Echtzeit und zur Aushändigung der aufbewahrten Randdaten des vergangenen Fernmeldeverkehrs verpflichten (rückwirkende Überwachung).

5 Die Anbieterinnen von Fernmeldediensten müssen die Randdaten des Fernmeldeverkehrs während 6 Monaten aufbewahren.

- Pflichten während des Pikettdienstes (Art. 11 Abs. 2 VÜPF)
- Art. 48 VÜPF

E. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste (normal) bei Auskünften

- Anbieterinnen abgeleiteter Kommunikationsdienste müssen dem Dienst die ihnen vorliegenden Angaben liefern (Art. 22 Abs. 3 BÜPF)
- Art. 11 Abs. 2 VÜPF
- Art. 18 Abs. 4 VÜPF

F. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste (normal) bei Überwachungen, Notsuchen und Fahndungen

- Duldungspflicht (Art. 27 Abs. 1 BÜPF)
- Art. 27 Abs. 2 BÜPF
- Art. 11 Abs. 2 VÜPF

G. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Auskunftspflichten (gross), bei Auskünften

Voraussetzung: Anbieterin bietet Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft an.

- sind den normalen FDA gleichgestellt
- liefern Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 BÜPF)
- müssen in der Lage sein, die Auskünfte gemäss Art. 31-44 VÜPF zu beantworten (Art. 18 Abs. 1 i.V. mit Art. 21 Abs. 4 VÜPF)
- Sofern die Abfrageschnittstelle des Verarbeitungssystems die automatische Beantwortung ausführen kann, beantworten sie die Auskunftsgesuche gemäss den Artikeln 33-40 automatisiert, jene gemäss den Artikeln 41-46 können sie auch manuell beantworten (Art. 18 Abs. 2 VÜPF).
- Aufbewahrungspflichten für die Daten gemäss Art. 22 BÜPF sowie Art. 20 VÜPF
- Art. 11 Abs. 2 VÜPF

H. Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste mit weitergehenden Überwachungspflichten (gross), bei Überwachungen, Notsuchen und Fahndungen

Voraussetzung: Anbieterin bietet Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft an.

- sind den normalen FDA gleichgestellt (Art. 27 Abs. 3 BÜPF)
- Pflichten während des Pikettdienstes (Art. 11 Abs. 2 VÜPF)
- erfüllen die Pflichten gemäss Art. 26 Abs. 1-5 BÜPF
- Art. 48 VÜPF