13.025

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

vom 27. Februar 2013

Sehr geehrte Frau Nationalratspräsidentin
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen den Entwurf für eine Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs.

Gleichzeitig beantragen wir Ihnen, die folgenden parlamentarischen Vorstösse abzuschreiben:

2007	M	06.3170	Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf den elektronischen Netzwerken (N 22.6.2007; S 11.12.2007, Schweiger Rolf)
2010	M	07.3627	Registrierungspflicht bei Wireless-Prepaid-Karten (N 3.6.2009, Glanzmann-Hunkeler Ida; S 18.3.2010)
2010	P	10.3097	Ermittlung von Internet-Straftätern (S 10.6.2010, Kommission für Rechtsfragen SR)
2011	M	10.4133	Verlängerung der Aufbewahrungspflicht für Protokolle über die Zuteilung von IP-Adressen (N 18.3.2011, Barthassat Luc; S 20.9.2011)
2012	M	10.3831	BÜPF-Revision (N 16. 3. 2012, Schmid-Federer Barbara; S 24. 9. 2012
2012	M	10.3876	BÜPF-Revision (N 16. 3. 2012, Eichenberger-Walther Corina; S 24. 9. 2012
2012	M	10.3877	BÜPF-Revision (N 16. 3. 2012, [von Rotz Christoph] Schwander Pirmin; S 24. 9. 2012
2012	P	11.4042	Überwachung mittels Trojanern (1) (N 28.2.2012, Kommission für Rechtsfragen NR)
2012	P	11.4043	Überwachung mittels Trojanern (2) (N 28.2.2012, Kommission für Rechtsfragen NR)
2012	P	11.4210	Kosten für die Überwachung des Fernmeldeverkehrs im Rahmen eines Strafverfahrens (S 5.3.2012, Recordon Luc)

Wir versichern Sie, sehr geehrte Frau Nationalratspräsidentin, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

27. Februar 2013

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ueli Maurer
Die Bundeskanzlerin: Corina Casanova

Übersicht

Mit der vorliegenden Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) soll sichergestellt werden, dass die notwendigen Überwachungen des Post- und Fernmeldeverkehrs weder heute noch in den kommenden Jahren durch die Verwendung neuer Technologien (wie etwa verschlüsselter Internettelefonie) verhindert werden können. Das Ziel besteht darin, nicht mehr, sondern besser überwachen zu können. Das BÜPF und die Strafprozessordnung (StPO) werden deshalb an die technische Entwicklung der letzten Jahre und, im Rahmen des Möglichen, an die künftigen Entwicklungen in diesem Bereich angepasst.

Ausgangslage

Die grossen technologischen Fortschritte der letzten Jahre im Bereich der Telekommunikation bieten den Benutzerinnen und Benutzern eine Vielzahl von Interaktionsmöglichkeiten. Diese werden in den allermeisten Fällen in legaler Weise genutzt. Allerdings können die neuen Technologien auch zur Begehung von Straftaten verwendet werden. Es hat sich gezeigt, dass der Gebrauch solcher Technologien – etwa im Bereich der verschlüsselten Internettelefonie – die Begehung von Straftaten. Daher müssen Instrumente bereitgestellt werden, um auch strafbare Handlungen aufklären zu können, die unter Verwendung solcher Technologien begangen worden sind.

Der Anwendung des schweizerischen Rechts sind jedoch auch weiterhin durch den Grundsatz der Territorialität Grenzen gesetzt, und eine effiziente Strafverfolgung in Fällen mit transnationalem Bezug (z.B. bei der Verwendung von E-Mail-Konten bei Anbietern mit Sitz im Ausland) ist somit erschwert. Die «virtuelle Globalisierung» stellt ein grundsätzliches Problem dar für die Rechtsanwendung im Bereich Internet, die sich mit der beantragten Totalrevision nicht lösen lässt.

Das Hauptziel der vorliegenden Totalrevision des BÜPF ist, die Überwachung von Personen zu ermöglichen, gegen die ein dringender Verdacht auf Begehung einer schweren Straftat besteht. Wie es bereits heute der Fall ist, soll es auch in Zukunft nicht möglich sein, ohne jeglichen Tatverdacht Bürgerinnen und Bürger zu überwachen oder gar präventive Überwachungen durchzuführen; die persönliche Freiheit bleibt gewahrt. Ein weiteres Ziel besteht darin, Überwachungen ausserhalb von Strafverfahren durchführen zu können, um vermissten Personen zu suchen oder nach geflohenen Personenfahnden zu können.

Die strafprozessualen Bestimmungen des BÜPF wurden in die Strafprozessordnung (StPO) überführt, die am 1. Januar 2011 in Kraft getreten ist. Die nun angestrebten Ziele der vorliegenden Revision des BÜPF erfordern daher nicht nur die Totalrevision dieses Gesetzes, sondern auch die Anpassung einiger Verfahrensbestimmungen in der StPO. Neue Überwachungsmöglichkeiten müssen auch in die StPO und in den Militärstrafprozess (MStP) aufgenommen werden.

Inhalt der Vorlage

Mit der vorliegenden Totalrevision wird die Struktur des BÜPF geändert und eine konsequente Systematik mit einer neuen Nummerierung eingeführt. Die Artikel werden genauer formuliert und ergänzt. Wichtige Fragen, die bisher nur auf Verordnungsstufe geregelt sind, werden neu in das Gesetz aufgenommen.

Folgende inhaltliche Anpassungen und Neuerungen sind vorgesehen:

- *Die Aufgaben des Dienstes für die Überwachung des Post- und Fernmeldeverkehrs werden geklärt und erweitert.*
- *Der persönliche Geltungsbereich wird erheblich ausgedehnt. Es gibt verschiedene Kategorien von Mitwirkungspflichtigen.*
- *Der Umfang der Mitwirkungspflicht wird für jede Kategorie entsprechend der spezifischen Tätigkeit abgestuft definiert.*
- *Die Daten aus Überwachungen werden zentral aufbewahrt, und der Zugang zu diesen Daten, die Einsichtnahme und die Aufbewahrungsdauer werden geregelt.*
- *Die Aufbewahrungspflicht für Randdaten wird von sechs auf zwölf Monate ausgedehnt.*
- *Es wird eine klare gesetzliche Grundlage für den Einsatz von besonderen technischen Überwachungsgeräten (wie z.B. IMSI-Catcher) und besonderen Informatikprogrammen («GovWare») geschaffen.*
- *Die Regelung zum Schutz des Berufsgeheimnisses wird angepasst.*
- *Wie es schon bisher der Fall ist, kann eine Überwachung angeordnet werden, um ausserhalb von Strafverfahreneine vermisste Person aufzufinden. Ferner ist es neu möglich, nach einer Person zu fahnden, gegen die eine Freiheitsstrafe oder eine freiheitsentziehende Massnahme verhängt wurde.*
- *Es werden spezifische Strafbestimmungen sowie eine Bestimmung bezüglich der administrativen Aufsicht eingeführt.*
- *Die Rechtsmittel gegen die Verfügungen des Dienstes und die zulässigen Rügen sind neu im Gesetz geregelt.*

Das heute geltende Gebühren- und Entschädigungssystem wird demgegenüber beibehalten.

Inhaltsverzeichnis

Botschaft

1 Grundzüge der Vorlage

1.1 Ausgangslage

Im Bereich der Telekommunikation, vor allem im Bereich des Internets, wurden in den letzten Jahren grosse technologische Fortschritte verzeichnet. Diese Fortschritte bieten den Benutzerinnen und Benutzern eine Vielzahl von Kommunikationsmöglichkeiten. Wie die klassischen Kommunikationsmittel können jedoch auch die neuen Technologien (insbesondere im Bereich des Internets) für illegale Zwecke genutzt werden. Dies gilt vor allem für die Bereiche Kinderpornografie, organisiertes Verbrechen und Betäubungsmittel. Zudem erleichtert die Vielfalt, die hohe Verfügbarkeit und die einfache Anwendung dieser Kommunikationstechnologien die Begehung von Straftaten.

Die technologische Entwicklung erschwert nicht nur die technische Durchführung der Überwachungen des Fernmeldeverkehrs, die Technologie kann auch den Gesetzgeber «überholen». So kann eine technisch zwar durchführbare Überwachung rechtlich problematisch oder sogar unzulässig sein, weil sie durch die gesetzliche Grundlage nicht mehr (klar) gedeckt ist. Beispiele für diese Rechtsunsicherheit sind die nach geltendem Recht fehlende Möglichkeit, reine Email-Provider zur Speicherung von Randdaten zu verpflichten, oder die Überwachung von verschlüsselter Kommunikation im Bereich Email und Internettelefonie, welche oft nur durch den – nach geltendem Recht höchst umstrittenen – Einsatz von besonderen Informatikprogrammen (GovWare) möglich ist. Daher muss dafür gesorgt werden, dass die Überwachungen, die zur Aufklärung strafbarer Handlungen notwendig sind, nicht durch die Verwendung neuer Technologien verhindert werden können. Dieses Ziel wird massgeblich durch die Ausdehnung des Bereichs der mitwirkungspflichtigen Anbieterinnen erreicht.

Der Anwendung des schweizerischen Rechts sind jedoch durch den Grundsatz der Territorialität der Gesetze Grenzen gesetzt. Eine rasche und effiziente Strafverfolgung ist somit in Fällen mit transnationalem Bezug (z.B. bei der Verwendung von E-Mail-Konten bei Anbietern im Ausland) erschwert, weil nur der Rechtshilfeweg offen steht. Die gewünschten Daten können in solchen Fällen oft nicht innert nützlicher Frist (oder gar nicht) beschafft werden. Der Entwurf ändert an dieser Tatsache nichts.

1.2 Die beantragte Neuregelung

Das Ziel der Totalrevision des Bundesgesetzes vom 6. Oktober 2000[1] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) besteht kurz gesagt in erster Linie darin, nicht mehr, sondern besser überwachen zu können. Es geht in erster Linie darum, die Überwachung von Personen zu ermöglichen, gegen die ein dringender Verdacht auf Begehung einer schweren Straftat besteht. Hingegen besteht kein Anlass, ohne Tatverdacht die Überwachung von Bürgerinnen und

1 SR **780.1**

Bürger zuzulassen oder präventive Überwachungen zu gestatten. Ausserhalb von Strafverfahren soll die Durchführung von Überwachungen einzig in Fällen zulässig sein, in denen vermisste oder verurteilte Personen gesucht werden.

Der Entwurf (E-BÜPF) klärt und ergänzt die Aufgaben des Dienstes für die Überwachung des Post- und Fernmeldeverkehrs (Dienst). Der persönliche Geltungsbereich des BÜPF wird erheblich ausgedehnt; der Umfang der Mitwirkungspflichten wird jedoch im Sinne der Verhältnismässigkeit für jede Kategorie entsprechend der spezifischen Tätigkeit abgestuft definiert. Für die Daten aus Überwachungen ist eine zentrale Langzeitaufbewahrung im Verarbeitungssystem des Dienstes vorgesehen.

Die Aufbewahrungspflicht für Randdaten wird von sechs auf zwölf Monate ausgedehnt und entsprechend auch der Zeitraum, in dem diese Daten für die Strafverfolgungsbehörden zur Verfügung stehen.

Das BÜPF regelt neu auch die straf- und verwaltungsrechtlichen Folgen, falls die mitwirkungspflichtigen Anbieterinnen ihren Pflichten nicht nachkommen. Es enthält zudem eine Bestimmung zu den Rechtsmitteln gegen die Verfügungen des Dienstes und den zulässigen Rügen.

Die strafprozessualen Bestimmungen des BÜPF wurden in die Strafprozessordnung (StPO)[2] überführt, die am 1. Januar 2011 in Kraft getreten ist . Die nun angestrebten Ziele erfordern deshalb nicht nur die Totalrevision des BÜPF, sondern auch die Revision einiger Verfahrensbestimmungen in der StPO. Zudem sollen zwei neue Überwachungsmöglichkeiten in der StPO geregelt werden. Damit bestehen klare gesetzliche Grundlagen für den zukünftigen Einsatz besonderer technischer Überwachungsgeräte (wie z.B. IMSI-Catcher) und besondere Informatikprogramme (sogenannte «GovWare»). Die Regelung zum Schutz des Berufsgeheimnisses wird ebenfalls angepasst. Sämtliche Änderungen wurden entsprechend auch im Militärstrafprozess vom 23. März 1979[3] (MStP) vorgenommen.

Auf diese verschiedenen Aspekte wird weiter unten detaillierter eingegangen (siehe Ziff. 1.4 und 2).

1.3 Entstehungsgeschichte

1.3.1 Auftrag des Bundesrates

Im März 2006 beauftragte der Bundesrat das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) und das Eidgenössische Justiz- und Polizeidepartement (EJPD) mit der Klärung der offenen Fragen, die sich in Bezug auf die Fernmeldeüberwachung zu Strafverfolgungszwecken und die Entschädigung der Fernmeldedienstanbieterinnen für ihre Aktivitäten im Rahmen dieser Überwachung stellen. Im Rahmen dieses Auftrags verfasste das Generalsekretariat des EJPD (GS EJPD) einen Bericht und führte darin die Bereiche auf, in denen eine Revision des BÜPF wünschenswert erschien. Im Mai 2007 erteilte das GS EJPD dem Bundesamt für Justiz (BJ) den Auftrag, einen Vorentwurf (VE-BÜPF) mit einem erläuternden Bericht zu erarbeiten.

2 SR **312.0**
3 SR **322.1**

1.3.2 Expertengruppe

Das BJ setzte im September 2008 eine Expertengruppe als beratendes Organ ein, dem Vertreterinnen und Vertreter der folgenden Behörden und Organisationen angehörten: Bundesanwaltschaft (BA), Bundeskriminalpolizei (BKP), Bundesamt für Kommunikation (BAKOM), Schweizerischer Verband der Telekommunikation (asut), kantonale Strafverfolgungsbehörden, Dienst Überwachung Post- und Fernmeldeverkehr im Informatik Service Center EJPD (Dienst) und BJ. Bei der Erarbeitung des VE-BÜPF berücksichtigte das BJ die Diskussionen, die diese Expertengruppe geführt hatte.

1.3.3 Vorentwurf und Vernehmlassungsverfahren

Am 19. Mai 2010 gab der Bundesrat den VE-BÜPF[4] und den erläuternden Bericht[5] in die Vernehmlassung, die bis zum 18. August 2010 lief. Sie richtete sich an alle Kantone, an die politischen Parteien, an die Organisationen, die im Bereich der Strafverfolgung oder der Telekommunikation tätig sind, sowie an mehrere andere interessierte Organisationen[6].

Beim EJPD gingen 106 Stellungnahmen ein, die insgesamt rund 700 Seiten umfassten. Geäussert haben sich sämtliche Kantone, sechs politische Parteien und 74 interessierte Organisationen. Die Antworten wurden in einem Bericht vom Mai 2011 zusammengefasst[7].

Von allen Vernehmlassungsteilnehmern anerkannt oder zumindest nicht bestritten wurde die Notwendigkeit, das BÜPF an die technische Entwicklung, die in den letzten Jahren stattgefunden hat, anzupassen. Zu den einzelnen vorgeschlagenen Bestimmungen wurden jedoch zahlreiche, zum Teil strukturelle und umfassende Vorbehalte angebracht. Teilweise wurde gar eine komplette Überarbeitung verlangt. Reaktionen lösten vor allem die folgenden Themen aus:

- Persönlicher Geltungsbereich. Etliche Teilnehmer unterstützten die geplante Ausdehnung. Viele lehnen sie hingegen ab oder verlangten eine Umformulierung von Artikel 2 Absatz 1 Buchstabe b VE-BÜPF, da dieser nicht klar sei oder zu weit gehe, insbesondere aufgrund seiner Tragweite und der wirtschaftlichen Auswirkungen auf die betroffenen Personen. Umstritten war auch die Frage, ob Anbieter wie die Webhoster (Hosting-Provider), die Internetdienstanbieterinnen darstellen, in den persönlichen Geltungsbereich des Gesetzes aufgenommen werden sollen.
- Zentrale Langzeitaufbewahrung der Überwachungsdaten im Verarbeitungssystem des Dienstes. Diese Art der Aufbewahrung wurde von mehreren Vernehmlassungsteilnehmern unterstützt. Sie verlangten jedoch teilweise erhebliche Anpassungen nach dem Vorbild des bisherigen Systems, insbesondere die Beibehaltung der postalischen Zustellung von nicht aus Internetüberwachungen stammenden Daten auf Datenträgern. Eine grössere Zahl

4 www.admin.ch/ch/d/gg/pc/documents/1719/Vorlage.pdf
5 www.admin.ch/ch/d/gg/pc/documents/1719/Bericht.pdf
6 www.admin.ch/ch/d/gg/pc/documents/1719/Adressatenliste.pdf
7 www.admin.ch/ch/d/gg/pc/documents/1719/Bericht_V_Ueberwachung_des_Post-und_Fernmeldeverkehrs.pdf

von Teilnehmern erachtete die vorgesehene Regelung als äusserst kompliziert und zog die Vereinbarkeit mit der StPO in Zweifel. Andere Teilnehmer stellten sich gegen die zentrale Aufbewahrung beim Dienst und lehnten den Online-Zugriff, auch für die beschuldigte Person und ihren Rechtsbeistand, aus sicherheitstechnischen Gründen ab.

– Fehlende Prüfungspflicht des Dienstes hinsichtlich der Rechtmässigkeit der Überwachungsanordnung. Zahlreiche Teilnehmer forderten, der Dienst sei zu verpflichten, die rechtliche Zulässigkeit der ihm übermittelten Überwachungsanordnungen zu überprüfen.

– Mitwirkungspflichten: Für eine Vielzahl von Teilnehmern waren die konkreten Pflichten zu wenig klar geregelt.

– Allgemeine Pflicht der Fernmeldedienstanbieterinnen, die Internet-Benutzerinnen und -Benutzer zu identifizieren. Eine grössere Anzahl Vernehmlassungsteilnehmer begrüsste diese Bestimmung, insbesondere im Zusammenhang mit der Benutzung von Systemen, die Hotels ihren Gästen zur Verfügung stellen, und dem Zugang zum Web über Internetcafés usw. Eine Vielzahl von Teilnehmern beantragte hingegen die Streichung oder Anpassung der Bestimmung, da diese Identifikationspflicht als unverhältnismässig oder unpraktikabel und unwirksam erachtet wird.

– Verlängerung der Aufbewahrungsfrist für Randdaten von sechs auf zwölf Monate. Grundsätzlich begrüssten zahlreiche Teilnehmer diese Verlängerung. Viele lehnten jedoch die entsprechende Bestimmung ab oder verlangten eine Überarbeitung der Regelung, denn diese Bestimmung ermögliche es, systematisch Daten unverdächtiger Personen während eines noch längeren Zeitraums auf Vorrat zu speichern. Zudem verursache die Verlängerung der Aufbewahrungsfrist hohe Kosten.

– Aufhebung der Entschädigung der Post- und Fernmeldedienstanbieterinnen. Mehrere Teilnehmer begrüssten die Streichung der Entschädigung, die sie als systemwidrig erachten. Zahlreiche Teilnehmer sprachen sich jedoch gegen die geplante Aufhebung aus. Sie betonten, die Strafverfolgung sei eine staatliche Aufgabe und daher durch das Gemeinwesen zu tragen. Einige Vernehmlassungsteilnehmer wiesen darauf hin, dass die Beschaffung einer teurer Infrastruktur notwendig werde, um die neuen gesetzlichen Anforderungen zu erfüllen, oder sie beantragten einer differenziertere Regelung.

– Rechtsmittel gegen die Überwachungsverfügungen des Dienstes. Eine grosse Zahl von Teilnehmern verlangte, die Möglichkeit für die mitwirkungspflichtigen Anbieterinnen ausdrücklich vorzusehen, die Rechtmässigkeit der durch den Dienst erlassenen Überwachungsverfügung von einem Gericht überprüfen zu lassen.

– Abfangen von Daten durch das Einführen von GovWare in fremde Datenverarbeitungssysteme. Eine bedeutende Zahl von Teilnehmern begrüsste die Möglichkeit, GovWare einzusetzen, vor allem weil das Problem der Datenverschlüsselung tendenziell stark zunehme. Eine grössere Teilnehmergruppe lehnte jedoch die Verwendung derartiger Informatikprogramme gänzlich ab oder brachte erhebliche Vorbehalte an. Dabei wurde insbesondere auf den massiven Eingriff in die Privatsphäre der Betroffenen hingewiesen, bei dem sämtliche Daten des betroffenen Datenverarbeitungssystems einsehbar seien

(Online-Durchsuchung). Genannt wurden auch die zu hohen Risiken für die Informatiksicherheit und für die Verlässlichkeit und Integrität der Beweismittel sowie die Forderung, diese Überwachungsart nur für einen Teil der Straftaten (die schwersten), die in Artikel 269 Absatz 2 StPO aufgeführt sind, zuzulassen.

1.3.4 Anpassungen nach der Vernehmlassung

Die Botschaft stützt sich auf die Vernehmlassungsversion des VE-BÜPF und berücksichtigt die wichtigsten fundierten Einwände, Bemerkungen und Vorschläge in den eingegangenen Stellungnahmen. Gegenüber dem VE-BÜPF wurden erhebliche, teilweise sogar grundlegende Änderungen vorgenommen.

Es erfolgten insbesondere die nachstehenden Anpassungen:

- Der persönliche Geltungsbereich des Gesetzes wurde genauer formuliert und auf verschiedene Kategorien von Personen und Anbieterinnen («Mitwirkungspflichtige») ausgedehnt; die Kategorien sind durch spezifische Tätigkeiten gekennzeichnet.
- Für die verschiedenen Kategorien von Mitwirkungspflichtigen wurden die jeweiligen Pflichten genauer formuliert und ergänzt. Dabei wurde der Umfang der Mitwirkungspflichten anhand der spezifischen Tätigkeit festgelegt.
- Das EJPD kann ein beratendes Organ einsetzen, um die reibungslose Durchführung der Überwachungen und die ständige Weiterentwicklung in diesem Bereich zu fördern. Dem Organ gehören Vertreterinnen und Vertreter der interessierten Kreise an.
- Für die zentrale Langzeitaufbewahrung der Überwachungsdaten im Verarbeitungssystem des Dienstes wurden für die Behörden – insbesondere für die Strafverfolgungsbehörden – zweckmässigere, einfachere und praktikablere Bestimmungen vorgesehen. Damit verringert sich auch der administrative Aufwand für den Dienst.
- Um die Abläufe effizienter zu gestalten, ist eine gesetzliche Grundlage für eine Schnittstelle vorgesehen, mit der sich die Überwachungsdaten aus dem vom Dienst betriebenen Verarbeitungssystem auf elektronischem Weg in eine Datenbank gemäss dem Bundesgesetz vom 13. Juni 2008[8] über die polizeilichen Informationssysteme des Bundes (BPI) kopieren lassen.
- Der Dienst kann die ihm übermittelten Überwachungsanordnungen einer umfassenderen materiellen Prüfung unter dem Gesichtspunkt des Verwaltungsrechts unterziehen. Stellt er dabei ein Problem fest, ist er verpflichtet, die anordnende Behörde und die Genehmigungsbehörde zu benachrichtigen. Mit dieser Bestimmung wird keine materielle Prüfung in Bezug auf strafprozessuale Gründe angestrebt.
- Auf eine allgemeine Pflicht der Fernmeldedienstanbieterinnen zur Identifikation der Internet-Nutzerinnen und -Nutzer wird verzichtet.

8 SR **361**

- Im Entwurf sind Bestimmungen vorgesehen, die sich auf die Einhaltung («Compliance») der Pflichten der Fernmeldedienstanbieterinnen bei der Durchführung der Überwachungen des Fernmeldeverkehrs beziehen. Auch die Folgen einer Nichteinhaltung dieser Pflichten sind geregelt.
- Auf die Aufhebung der Entschädigung der Anbieterinnen von Post- und Fernmeldediensten wird verzichtet.
- Für die Verfolgung und Beurteilung der im BÜPF geregelten Straftaten ist der Dienst zuständig; das Bundesgesetz vom 22. März 1974[9] über das Verwaltungsstrafrecht (VStrR) ist anwendbar.
- Die Mitwirkungspflichtigen können die Rechtmässigkeit der vom Dienst erlassenen Überwachungsverfügungen durch ein Gericht überprüfen lassen.
- Das Abfangen von Daten aus dem Fernmeldeverkehr durch das Einführen von GovWare in fremde Datenverarbeitungssysteme soll bei Straftaten zulässig sein, bei denen eine verdeckte Ermittlung zulässig wäre (vgl. den Katalog in Art. 286 Abs. 2 StPO). Der umfangreichere Straftatenkatalog, bei dem eine Post- und Fernmeldeüberwachung möglich ist (vgl. Art. 269 Abs. 2 StPO), soll beim Einsatz von GovWare nicht zur Anwendung gelangen.

1.4 Die wichtigsten Änderungen

1.4.1 Persönlicher Geltungsbereich

Der persönliche Geltungsbereich des BÜPF wird erheblich erweitert; er umschreibt, wer dem Gesetz unterstellt ist, d.h. wem daraus Pflichten erwachsen. Nach geltendem Recht umfasst der persönliche Geltungsbereich des BÜPF nur die Anbieterinnen von Post- oder Fernmeldediensten, zu denen auch die Internetzugangsanbieterinnen gehören, sowie die Betreiberinnen von internen Fernmeldenetzen und Hauszentralen. Daneben können jedoch auch weitere Personen oder Unternehmen Daten im Zusammenhang mit dem Post- oder Fernmeldeverkehr besitzen, welche die Strafverfolgungsbehörden allenfalls benötigen. Angesichts der oben dargestellten aktuellen Probleme wurde der persönliche Geltungsbereich im Entwurf genauer formuliert; dieser umfasst nun sechs verschiedene Kategorien von Personen («Mitwirkungspflichtige»), die durch spezifische Tätigkeiten gekennzeichnet sind. Erfasst werden sollen:

- die Anbieterinnen von Postdiensten (Die Schweizerische Post, Kuriere etc.);
- die Anbieterinnen von Fernmeldediensten (z.B. klassische Telefonanbieterinnen);
- die Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen («Anbieterinnen abgeleiteter Kommunikationsdienste», z.B. reine Email-Provider);
- die Betreiberinnen von internen Fernmeldenetzen (z.B. unternehmensinterne Netzwerke, «Intranet»);
- die Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen (z.B. Hotels oder Internet-Cafés);

9 SR **313.0**

– die professionellen Wiederverkäufer von Karten und ähnlichen Mitteln (Prepaid-Karten etc.), die den Zugang zu einem öffentlichen Fernmeldenetz ermöglichen.

Der Umfang der Mitwirkungspflichten wird jedoch im Sinne der Verhältnismässigkeit für jede Kategorie gesondert definiert (siehe Ziff. 1.4.6).

Für Einzelheiten siehe die Erläuterungen zu Artikel 2.

1.4.2 Beratendes Organ

Das EJPD kann ein beratendes Organ einsetzen, um die reibungslose Durchführung der Überwachungen des Post- und Fernmeldeverkehrs und die ständige Weiterentwicklung in diesem Bereich zu fördern. Dieses Organ setzt sich aus Vertreterinnen und Vertretern der verschiedenen Akteure zusammen (EJPD, Dienst, Kantone, Strafverfolgungsbehörden und Anbieterinnen von Post- und Fernmeldediensten). Da diese Akteure teilweise gegenläufige Interessen verfolgen, ist es – wie die Erfahrung gezeigt hat – äusserst wichtig, dass sie in einem Organ zusammenarbeiten. Diese schon heute auf informeller Grundlage bestehende Zusammenarbeit ist bisher gesetzlich nicht geregelt.

Für Einzelheiten siehe die Erläuterungen zu Artikel 5.

1.4.3 Zentrale Langzeitaufbewahrung der Überwachungsdaten

Nach geltendem Recht übermittelt der Dienst alle Daten, die durch die Überwachung des Fernmeldeverkehrs gesammelt werden, auf Datenträgern per Post an die (Strafverfolgungs-)Behörden. Sobald diese dem Dienst den Empfang bestätigt haben, löscht er die Daten in seinem System. Die Daten werden, wie alle anderen Beweismittel, in den Gerichtsakten aufbewahrt.

Neu ist vorgesehen, die Überwachungsdaten über einen längeren Zeitraum zentral im Verarbeitungssystem des Dienstes aufzubewahren. Dies gilt für sämtliche Daten, die aus Überwachungen des Fernmeldeverkehrs hervorgehen, für die Daten aus klassischen Telefonüberwachungen sowie für Daten, die aus Internetüberwachungen stammen. Für diese Anpassung spricht vor allem die Tatsache, dass die Datenbestände, namentlich jene aus den Internetüberwachungen, immer umfangreicher werden. Dies führt dazu, dass es immer aufwendiger wird, diese Daten auf Datenträgern per Post zu befördern. Ausserdem wird es zunehmend schwierig, diese Datenträger aufzubewahren und zu verwalten.

Bei der neuen Betriebsweise können die (Strafverfolgungs-)Behörden die Daten zu den Verfahren, mit denen sie befasst sind, über einen Online-Zugriff auf das Verarbeitungssystem des Dienstes abrufen. Auch die Parteien, einschliesslich der beschuldigten Person und ihres Anwalts, können online auf die Daten zugreifen. Unter bestimmten Bedingungen können die Daten wie bisher auf mobilen Datenträgern übermittelt werden.

Für Einzelheiten siehe die Erläuterungen zu den Artikeln 6–14.

1.4.4 Schnittstelle zwischen dem Informatiksystem des Dienstes und dem polizeilichen Informationssystem-Verbund des Bundesamtes für Polizei

Der polizeiliche Informationssystem-Verbund des Bundesamtes für Polizei dient diesem und den kantonalen Polizeibehörden vor allem zur Auswertung der Informationen, die im Rahmen von Strafuntersuchungen beschafft wurden. Die elektronische Übertragung der Daten aus dem Informatiksystem des Dienstes in den polizeilichen Informationssystem-Verbund gemäss Artikel 10, 12 und 13 BPI bietet gegenüber der «manuellen» Übertragung mehrere Vorteile. Unter anderem kann so Zeit und Geld gespart und eine höhere Datensicherheit erreicht werden (verringertes Risiko von Datenverlusten und verringertes Risiko von Fehlern, die sich negativ auf die Datenqualität auswirken können). Die elektronische Übertragungsart darf keinesfalls dazu führen, dass die Zugriffsregeln auf das Informatiksystem des Dienstes und diejenigen auf das Informationssystem gemäss BPI unterwandert werden.

Für Einzelheiten siehe die Erläuterungen zu Artikel 14.

1.4.5 Materielle Prüfung der Überwachungsanordnungen durch den Dienst

Zusätzlich zur bereits im geltenden Recht vorgesehenen formellen Prüfung kann der Dienst die ihm übermittelten Überwachungsanordnungen neu einer materiellen Prüfung unter dem Gesichtspunkt des Verwaltungsrechts unterziehen. Stellt er dabei ein Problem fest, ist er verpflichtet, die anordnende Behörde (in der Regel die Staatsanwaltschaft) und die Genehmigungsbehörde (in der Regel das Zwangsmassnahmengericht) zu benachrichtigen. Der Dienst kann prüfen, ob die übermittelte Überwachungsanordnung in der Gesetzgebung vorgesehen, technisch geeignet und durchführbar ist. Eine materielle Prüfung in Bezug auf strafprozessuale Gründe ist dem Dienst hingegen verwehrt; für diese Prüfung ist die Genehmigungsbehörde zuständig.

Die anordnende Behörde und die Genehmigungsbehörde können die Meinung des Dienstes berücksichtigen und die Anordnung widerrufen oder sie nicht genehmigen; sie sind aber nicht dazu verpflichtet. Dieser Mechanismus verhindert, dass der Dienst die Durchführung einer problematischen Überwachungsanordnung «blind» verfügen muss und die problematischen Punkte erst auf Beschwerde der betroffenen Anbieterin hin gerichtlich überprüft werden. Zahlreiche Probleme können so schon im Vorfeld und auf unkomplizierte Weise geklärt werden. Ein besonderes Rechtsmittel, um Divergenzen zwischen dem Dienst und der anordnenden Behörde gerichtlich zu klären, ist jedoch nicht notwendig. Ein solches Rechtsmittel ist angesichts des erweiterten Rechtsschutzes der Mitwirkungspflichtigen entbehrlich.

Für Einzelheiten siehe die Erläuterungen zu Artikel 16 Buchstabe b.

1.4.6 Mitwirkungspflichten

Die Mitwirkungspflichten sind im geltenden BÜPF zu wenig klar geregelt. Mit Rücksicht auf den technischen Fortschritt müssen die Mitwirkungspflichtigen zudem zusätzliche Leistungen erbringen.

Für die verschiedenen Kategorien von Mitwirkungspflichtigen wurden daher in den Artikeln 26–30 die Pflichten systematisiert, genauer formuliert und ergänzt und anhand der spezifischen Tätigkeit festgelegt.

Angesichts der technischen Materie ist es nicht angebracht, die Pflichten im Gesetz detailliert festzulegen. Die Einzelheiten werden vom Bundesrat auf dem Verordnungsweg geregelt, wofür sich – wie nach geltendem Recht – die Verordnung vom 31. Oktober 2001[10] über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) anbietet. Unter gewissen Bedingungen kann der Bundesrat einzelne Fernmeldedienstanbieterinnen von bestimmten Pflichten entbinden; er kann aber auch bestimmten Mitwirkungspflichtigen (z.B. Email-Providern) alle oder einen Teil der umfangreicheren Pflichten der Fernmeldedienstanbieterinnen auferlegen.

Die technischen und administrativen Ausführungsbestimmungen, mit denen die ordnungsgemässe und möglichst kostengünstige Ausführung der üblichen Überwachungstypen sichergestellt werden soll, werden nicht mehr wie bisher in Weisungen des Dienstes, sondern in Verordnungen des EJPD geregelt.

Aus Gründen der Praktikabilität wird darauf verzichtet, für die Anbieterinnen von Fernmeldediensten eine allgemeine Pflicht zur Identifikation der Internet-Nutzerinnen und -Nutzer vorzusehen, obwohl damit eine Lücke in der Überwachung zugelassen wird.

Für Einzelheiten siehe die Erläuterungen zu den Artikeln 19–30.

1.4.7 Verlängerung der Aufbewahrungsfrist für Randdaten und des Zeitraums, in dem diese verlangt werden können

Im Gegensatz zu den Inhaltsdaten enthalten Randdaten keine Angaben zum Inhalt der Postsendung oder der Fernmeldekommunikation, sondern nur zur Tatsache, wer wann wo mit wem usw. in Briefwechsel bzw. Verbindung stand. Im Hinblick auf eine wirksamere Verfolgung von Straftaten ist vorgesehen, die Aufbewahrungsfrist für die Randdaten von sechs auf zwölf Monate zu verlängern. Diese Daten werden auf «Vorrat» für allfällige künftige Strafuntersuchungen aufbewahrt und sind zur Bekämpfung der Kriminalität unerlässlich. Randdaten dürfen nicht präventiv, sondern grundsätzlich nur im Rahmen eines Strafverfahrens mit Zustimmung der Genehmigungsbehörde beschafft werden.

Die vorgesehene Verlängerung steht in Zusammenhang mit den Forderungen der Motionen Schweiger 06.3170 (Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf elektronischen Netzwerken) und Barthassat 10.4133 (Verlängerung der Aufbewahrungspflicht für Protokolle über die Zuteilung von IP-Adressen). Die in den Motionen aufgeworfene Problematik betrifft aber nicht nur Randdaten aus dem Fernmeldeverkehr, sondern auch solche aus dem Postverkehr. Die Erfahrungen der

10 SR **780.11**

Strafverfolgungsbehörden haben gezeigt, dass die Aufbewahrungsfrist für Randdaten nach geltendem Recht (d.h. sechs Monate) zu kurz bemessen ist: Oft ist diese Frist bereits vollständig oder grösstenteils abgelaufen, wenn die Behörde in der Lage ist, eine Überwachung anzuordnen.

Für Einzelheiten siehe die Erläuterungen zu den Artikeln 19 Absatz 4 und 26 Absatz 5 sowie 273 Absatz 3 StPO und 70*d* Absatz 3 MStP.

1.4.8 Informationen über Art und Merkmale von Dienstleistungen

Um die korrekte Durchführung der Überwachungen sicherzustellen, muss der Dienst auch die Schwierigkeiten voraussehen, die bei zukünftigen Überwachungen auftreten könnten. Er sollte nicht erst auf Probleme reagieren müssen, die sich bei der Durchführung einer neuen Überwachung stellen. Deshalb sollen die Anbieterinnen von Fernmeldediensten dem Dienst auf Verlangen darlegen, welche Dienstleistungen sie auf den Markt gebracht haben oder innerhalb von sechs Monaten auf den Markt bringen wollen und wozu diese dienen. Die Mitarbeiterinnen und Mitarbeiter des Dienstes unterstehen selbstverständlich dem Amtsgeheimnis (Art. 320 StGB).

Für Einzelheiten siehe die Erläuterungen zu Artikel 25.

1.4.9 Einhaltung der Pflichten und Folgen der Nichteinhaltung («Compliance»)

Um eine ordnungsgemässe Ausführung der Überwachungen sicherzustellen, enthält das Gesetz neu Bestimmungen zur Einhaltung der Pflichten der Fernmeldedienstanbieterinnen, und es regelt die Folgen der Nichteinhaltung dieser Pflichten («Compliance»). Die Bestimmungen beziehen sich vor allem auf die Fähigkeit, Auskünfte zu erteilen und die Überwachungen durchzuführen. Die Anbieterinnen können die Ausführung ihrer Aufgaben (teilweise oder gesamthaft) auf eigene Kosten an Dritte übertragen können; sie bleiben jedoch an die entsprechenden Pflichten gebunden.

Die Bestimmungen beziehen sich auch auf den Nachweis der Fähigkeit zur Auskunftserteilung und Überwachung. Zudem regeln sie die finanziellen Folgen für den Fall, dass eine unzureichende Überwachungsbereitschaft besteht.

Für Einzelheiten siehe die Erläuterungen zu den Artikeln 31–34.

1.4.10 Überwachungen ausserhalb von Strafverfahren

Nach Artikel 3 des geltenden BÜPF beschränkt sich die Überwachung des Post- und Fernmeldeverkehrs bei der Notsuche nach einer vermissten Person auf die Herausgabe der Randdaten. Neu soll es möglich sein, auch den Inhalt der Sendungen im Postverkehr sowie der Kommunikation im Fernmeldeverkehr zu beschaffen, weil auch diese Informationen Hinweise auf den Ort liefern können, an dem sich die vermisste Person befindet. Die Überwachung wird subsidiär zu den anderen Massnahmen angeordnet, die ergriffen werden können, um die gesuchte Person aufzufinden. Der Einsatz technischer Überwachungsgeräte (IMSI-Catcher, vgl. Art. 269bis

StPO) ist ebenfalls gestattet, jedoch nur subsidiär zu den oben erwähnten Suchmassnahmen. Mit dieser Überwachungsart lässt sich eine vermisste Person möglicherweise selbst dann auffinden, wenn sich die klassischen Massnahmen der Fernmeldeüberwachung als unwirksam erwiesen haben. Sollte dies notwendig sein, so kann nach Artikel 3 Absatz 1 des geltenden BÜPF nicht nur der Post- und Fernmeldeverkehr der gesuchten Person, sondern auch jener einer unbeteiligten Drittperson überwacht werden. Dies bleibt weiterhin möglich.

Eine Überwachung im eben beschriebenen Sinn soll auch erfolgen können, um nach einer Person zu fahnden, gegen die eine Freiheitsstrafe oder eine freiheitsentziehende Massnahme verhängt wurde. Die Überwachung ist im Rahmen eines laufenden Strafverfahrens zulässig; umso mehr muss sie zulässig sein, wenn nicht bloss ein dringender Verdacht besteht (Art. 269 Abs. 1 Bst. a StPO), sondern ein rechtskräftiges, vollstreckbares Urteil vorliegt.

Für die Überwachungen ausserhalb von Strafverfahren gilt das Verfahren nach den Artikeln 274–279 StPO grundsätzlich sinngemäss.

Für Einzelheiten siehe die Erläuterungen zu den Artikeln 35–37 sowie Ziffer 1.4.14.

1.4.11 Strafbestimmungen

Mit der vorliegenden Revision sollen Bestimmungen eingeführt werden, die eine Bestrafung ermöglichen, falls bestimmte Pflichten nicht erfüllt und dadurch Überwachungen behindert werden. Diese Bestrafung soll jedoch nur subsidiär zu strengeren Strafbestimmungen erfolgen, die gleichzeitig erfüllt sein könnten. Zu denken ist hier etwa an Strafbestimmungen zum Schutz des Amtsgeheimnisses (Art. 320 StGB) oder des Post- und Fernmeldegeheimnisses (Art. 321ter StGB) oder an Begünstigung (Art. 305 StGB). Die Erfahrung hat gezeigt, dass die grossen Anbieterinnen von Fernmeldediensten sich ihrer Pflichten grundsätzlich bewusst sind und diesen auch nachkommen.

Werden Anweisungen des Dienstes nicht befolgt, so muss eine Strafnorm anwendbar sein, die den Mechanismus von Artikel 292 StGB übernimmt. Angesichts der Einsparungen, die eine mitwirkungspflichtige Person erzielen kann, wenn sie den Anweisungen des Dienstes nicht Folge leistet, dürfte jedoch die in Artikel 292 StGB angedrohte Busse von maximal CHF 10 000.– allerdings nicht abschreckend wirken. Eine spezifische Bestimmung, die eine schwerere Strafe vorsieht, ist deshalb gerechtfertigt.

Aufgrund der Motion Schweiger 06.3170 (Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf elektronischen Netzwerken) wird eine weitere Strafbestimmung eingeführt, welche die Verletzung der Aufbewahrungspflicht für die Randdaten mit Strafe bedroht. Geahndet wird ausserdem die Verletzung von Dokumentationspflichten (insbesondere Aufzeichnung von Personen- bzw. Kundendaten) bei der Abgabe von Karten oder ähnlichen Mitteln, die den Zugang zu einem Fernmeldenetz ohne Abonnementsverhältnis ermöglichen (zum Beispiel mittels Prepaid-SIM-Karten). Die Erfahrung zeigt, dass eine solche Sanktion notwendig ist, um

diese Dokumentationspflichten durchzusetzen[11]. Wie dies bereits im geltenden BÜPF der Fall ist, wird ebenfalls bestraft, wer die Überwachung gegenüber Dritten nicht geheim hält.

Für die Verfolgung und Beurteilung der oben genannten Straftaten ist der Dienst zuständig; dafür sprechen mehrere Gründe: Zunächst erhält der Dienst am ehesten Kenntnis, dass eine solche strafbare Handlung begangen worden sein könnte. Auch bedroht Artikel 39 die Nichtbefolgung der Anweisungen des Dienstes mit Strafe. Zudem überträgt das BÜPF dem Dienst Aufgaben im Bereich der administrativen Aufsicht. Schliesslich erfordern die Verfolgung und Beurteilung dieser Straftaten spezifische technische Kenntnisse, über die der Dienst eher verfügen dürfte als die Strafverfolgungsbehörden der Kantone.

Diese Straftaten werden somit entsprechend der Zuständigkeit des Dienstes nach dem VStrR verfolgt und beurteilt.

Für Einzelheiten siehe die Erläuterungen zu den Artikeln 39 f.

1.4.12 Administrative Aufsicht

Es soll sichergestellt werden, dass nur jene dem BÜPF unterstellten Personen und Unternehmen tätig sein dürfen, die sich an die Vorschriften zur Überwachung des Post- und Fernmeldeverkehrs halten. Im Hinblick darauf wird Artikel 58 des Fernmeldegesetzes vom 30. April 1997[12] (FMG) teilweise für sinngemäss anwendbar erklärt. Bei einer Verletzung der Vorschriften zur Überwachung des Post- und Fernmeldeverkehrs kann der Dienst somit eine Mahnung aussprechen. Es wird zudem ein System von administrativen Sanktionen eingeführt, das sich vom System der strafrechtlichen Sanktionen unterscheidet und dieses ergänzt (siehe Ziff. 1.4.11). Gegenüber den Mitwirkungspflichtigen übt der Dienst seine Überwachungskompetenzen mit bindender Wirkung aus. Dies gilt jedoch nicht gegenüber den anordnenden Behörden und den Genehmigungsbehörden, da der Dienst gegenüber diesen Behörden keine Entscheidungsbefugnis besitzt (siehe Ziff. 1.4.5).

Für Einzelheiten siehe die Erläuterungen zu Artikel 41.

1.4.13 Rechtsmittel gegen die Überwachungsverfügungen des Dienstes

Das geltende BÜPF enthält keine Bestimmung zu den Rechtsmitteln gegen die Verfügungen des Dienstes; anwendbar ist einzig Artikel 32 der geltenden VÜPF.

Aus Gründen der Klarheit und der Rechtssicherheit soll im Gesetz neu eine Bestimmung eingeführt werden, die den Rechtsschutz gegen die Verfügungen des Dienstes regelt. Die Bestimmung übernimmt die bisher geltenden Grundsätze. Danach können die Mitwirkungspflichtigen die Rechtmässigkeit der vom Dienst erlassenen Überwachungsverfügung durch ein Gericht überprüfen lassen, dabei jedoch keine

11 Thomas Hansjakob, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2. Aufl., St. Gallen 2006, Art. 19*a* VÜPF N 2.

12 SR **784.10**

strafprozessualen Gründe geltend machen (wie etwa, ob ein dringender Verdacht nach Art. 269 Abs 1 Buchstabe a StPO vorliegt oder ob die Voraussetzungen für die Überwachung einer Drittperson nach Art. 270 Bst. b StPO gegeben sind).

Da bei einer Überwachung oft Dringlichkeit besteht, kommt der Beschwerde gegen eine Überwachungsverfügung des Dienstes keine aufschiebende Wirkung zu. Die Beschwerdeinstanz kann jedoch der Beschwerde aufschiebende Wirkung verleihen.

Für Einzelheiten siehe die Erläuterungen zu Artikel 42.

1.4.14 Einsatz von technischen Überwachungsgeräten

Die Ergänzung der StPO (und des MStP) soll der Staatsanwaltschaft (und dem militärischen Untersuchungsrichter) ermöglichen, Geräte wie IMSI-Catcher breiter einzusetzen, um mobile Kommunikationsgeräte (nicht nur Mobiltelefone) und mithin ihre Benutzerinnen und Benutzer zu identifizieren. Diese Nutzung des IMSI-Catchers kommt somit zu den bestehenden Möglichkeiten hinzu, Gespräche abzuhören und aufzuzeichnen und die erwähnten Geräte oder Benutzerinnen und Benutzer zu orten. Die Ergänzung ist für die Verfolgung von Straftaten notwendig. Zudem stellt die Identifikation im Vergleich zur Ortung sowie des Abhörens und Aufzeichnens von Gesprächen einen weniger starken Eingriff in die Privatsphäre dar[13].

Als Massnahme zur Überwachung des Fernmeldeverkehrs nach Artikel 269 StPO muss der von der Staatsanwaltschaft angeordnete Einsatz vom Zwangsmassnahmengericht genehmigt werden.

Für Einzelheiten siehe die Erläuterungen zu Artikel 269bis StPO sowie zu Artikel 70bis MStP.

1.4.15 Einsatz von Government Software

Der Entwurf ergänzt die StPO (und den MStP) durch eine ausdrückliche gesetzliche Grundlage, die der Staatsanwaltschaft (und dem militärischen Untersuchungsrichter) in einem Strafverfahren – nicht jedoch präventiv – unter ganz bestimmten Bedingungen (unter anderem mit der Genehmigung des Zwangsmassnahmengerichts) den Einsatz von Informatikprogrammen ermöglicht, die gewöhnlich als GovWare bezeichnet werden. Die GovWare soll nur subsidiär zu den klassischen Überwachungsmassnahmen eingesetzt werden, wobei selbstverständlich der Grundsatz der Verhältnismässigkeit gewahrt bleiben muss.

Die GovWare wird in ein Datenverarbeitungssystem eingeführt, um den Inhalt der Kommunikation und die Randdaten abzufangen. Dies ist jedoch nur zulässig bei Straftaten, bei denen eine verdeckte Ermittlung zulässig wäre (vgl. den Katalog in Art. 286 Abs. 2 StPO). Der umfangreichere Straftatenkatalog, bei dem eine Post- und Fernmeldeüberwachung möglich ist (vgl. Art. 269 Abs. 2 StPO), soll beim Einsatz von GovWare nicht zur Anwendung gelangen. Selbstverständlich muss die GovWare ohne Wissen der überwachten Person eingeschleust werden. Diese Über-

13 Sophie de Saussure, Le IMSI-Catcher: fonctions, applications pratiques et légalité, Jusletter 30.11.2009, Rz. 45–56 und 70.

wachungsmethode erfordert keine Mitwirkung einer Fernmeldedienstanbieterin. Dem Dienst kommt beim Einsatz von GovWare keine besondere Aufgabe zu.

Mit dieser Methode können nicht nur die Daten im Zusammenhang mit der Internettelefonie und dem E-Mail-Verkehr beschafft werden, sondern alle Daten aus dem Fernmeldeverkehr, der auch den Internetverkehr umfasst. Als «Datenverarbeitungssystem» gilt jedes Gerät, das den Fernmeldeverkehr über das Telefonnetz oder auf einem anderen Weg ermöglicht, zum Beispiel ein (mobiler) Computer oder ein Mobiltelefon.

Die Online-Durchsuchung eines Datenverarbeitungssystems mittels GovWare, mit der auf sämtliche persönlichen Daten (zum Beispiel Dokumente, Fotos) zugegriffen werden kann, soll verboten sein. Ausgeschlossen ist auch der Einsatz der GovWare, um die Kamera oder das Mikrofon eines Computers zu einem anderen Zweck als zur Überwachung des Fernmeldeverkehrs zu nutzen, zum Beispiel zur Überwachung eines Raumes.

Vereinzelt haben die Strafverfolgungsbehörden (Bund und Kantone) bereits früher GovWare gestützt auf die Strafprozessbestimmungen eingesetzt, die vor dem Inkrafttreten der StPO galten. In der Frage, ob der Einsatz von GovWare nach dem geltenden Recht zulässig ist, gehen die Meinungen auseinander; mehrheitlich wird die Zulässigkeit abgelehnt[14]. Es erscheint deshalb notwendig, eine ausdrückliche gesetzliche Grundlage zu schaffen, wenn GovWare zu den oben genannten Zwecken und Bedingungen eingesetzt werden soll.

Für Einzelheiten siehe die Erläuterungen zu Artikel 269ter StPO sowie zu Artikel 70ter MStP.

1.4.16 Sperrung des Zugangs zu Fernmeldediensten

Der Entwurf sieht vor, dass die Fernmeldedienstanbieterinnen unter bestimmten Voraussetzungen dazu verpflichtet werden, den Zugang zur Telefonie und zum Internet für gewisse Kunden zu sperren. Damit soll dazu beigetragen werden, die Personen zu identifizieren, die diese Dienste ohne Abonnementsverhältnis in Anspruch nehmen (z.B. durch Benutzung von Prepaid-SIM-Karten).

Für Einzelheiten siehe die Erläuterungen zu Artikel 6*a* FMG.

1.4.17 Vergleich mit dem ausländischen, vor allem mit dem europäischen Recht

In den Nachbarländern der Schweiz bestehen ähnliche Regelungen für die Überwachung des Post- und Fernmeldeverkehrs wie jene, die Gegenstand dieses Entwurfs sind. Allerdings lassen sich auch einige Unterschiede feststellen.

14 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 16; anderer Ansicht Sylvain Métille, a.a.O., Rz. 37.

Bezüglich der Randdaten ist in erster Linie die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006[15] zu nennen. Diese sieht für diese Daten eine Aufbewahrungsdauer von mindestens sechs Monaten und grundsätzlich höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation vor.

In Deutschland ist der Einsatz von Geräten wie IMSI-Catchern gestattet. Stark umstritten ist hingegen die Frage, ob die Überwachung von Fernmeldedaten mittels GovWare im Rahmen eines Strafverfahrens gesetzlich zulässig ist. Allerdings ist der Einsatz von GovWare unter ganz bestimmten Bedingungen zulässig, um präventiv eine Online-Durchsuchung vorzunehmen, die grundsätzlich die Überwachung von Fernmeldedaten abdeckt. Die vorgesehene Aufbewahrung der Randdaten während sechs Monaten ab dem Zeitpunkt der Kommunikation ist ebenfalls umstritten. Das deutsche Bundesverfassungsgericht hat die Bestimmungen zur Aufzeichnung dieser Daten für rechtswidrig erklärt, nicht jedoch den Grundsatz der Aufbewahrung der Daten, sofern deren Verwendung nur im Zusammenhang mit den schwersten Straftaten möglich ist.

In Österreich beträgt die Frist für die Aufbewahrung der Randdaten sechs Monate ab dem Zeitpunkt der Kommunikation. Die Verwendung von IMSI-Catchern ist ebenfalls gestattet. Die österreichische Regierung hat die Absicht geäussert, eine Rechtsgrundlage zu schaffen, damit in bestimmten Fällen eine Online-Durchsuchung – die grundsätzlich die Überwachung von Fernmeldedaten abdeckt – mittels GovWare durchgeführt werden kann. In den vergangenen Monaten befasste sich das österreichische Parlament mit dem entsprechenden Entwurf.

In Frankreich beträgt die Frist für die Aufbewahrung der Randdaten zwölf Monate ab dem Zeitpunkt der Kommunikation. Der Einsatz von IMSI-Catchern ist zulässig. Auch die Online-Durchsuchung im oben genannten Sinn unter Einsatz von GovWare ist unter bestimmten Voraussetzungen gestattet.

In Italien beträgt die Frist für die Aufbewahrung der Randdaten je nach Datentyp 12 bis 24 Monate ab dem Zeitpunkt der Kommunikation. Der Einsatz von IMSI-Catchern und von GovWare scheint nicht ausdrücklich geregelt zu sein.

15 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, Amtsblatt Nr. L 105 vom 13.04.2006 S. 54.

1.5 Abschreibung parlamentarischer Vorstösse

Auf die noch hängigen parlamentarischen Vorstösse im Zusammenhang mit der Revision des BÜPF[16] wird unter den einzelnen Bestimmungen der Vorlage eingegangen. Der Bundesrat beantragt die Abschreibung dieser Vorstösse.

2 Erläuterungen zu den einzelnen Artikeln

2.1 1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Sachlicher Geltungsbereich

Artikel 1 legt den sachlichen Geltungsbereich des BÜPF fest.

Absatz 1 erfährt gegenüber der Fassung im geltenden Recht keine wesentlichen Änderungen. Der sachliche Geltungsbereich umfasst die Überwachung des Postverkehrs. Zudem umfasst er die Überwachung des Fernmeldeverkehrs im Sinne von Artikel 269 Absatz 1 StPO sowie gemäss der Definition des Begriffs des Fernmeldewesens in den Artikeln 2 und 3 Buchstabe c FMG. Der Internetverkehr, der namentlich den E-Mail-Verkehr einschliesst[17], ist eine besondere Art des Fernmeldeverkehrs. Seine Überwachung fällt somit in den sachlichen Geltungsbereich des BÜPF. Die Internettelefonie gehört zum Internetverkehr und ist selbstverständlich ebenfalls Fernmeldeverkehr. Auch ihre Überwachung fällt deshalb in diesen Geltungsbereich. Bei der Frage, ob eine Überwachung zulässig ist, kann es nicht darauf ankommen, welche Übertragungswege und welche Technologien eingesetzt werden. Die Internettelefonie fällt wie die konventionelle Telefonie unter das Fernmeldegeheimnis nach Artikel 43 FMG. Artikel 269 StPO enthält die Rechtsgrundlage für die Aufhebung dieses Geheimnisses zum Zweck der Beweiserhebung im Rahmen eines Strafverfahrens[18].

16 Vgl. unten Ziff. 2.4, 2.6 und 2.10 (ad Art. 19, 26 und 39) ad 06.3170 Mo. Schweiger Rolf: Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf elektronischen Netzwerken, 24.3.2006; Ziff. 2.1 und 2.6 (ad Art. 2, 21, 26, 28 und 29) ad 07.3627 Mo. Glanzmann-Hunkeler Ida: Registrierungspflicht bei Wireless-Prepaid-Karten, vom 3.10.2007; Ziff. 2.6 (ad Art. 26) ad 10.4133 Mo. Barthassat Luc: Verlängerung der Aufbewahrungspflicht für Protokolle über die Zuteilung von IP-Adressen, vom 17.12.2010; Ziff. 2.2, 2.3, 2.6, 2.9 und 2.12 (ad Art. 6–18, 26 und 38, Art. 269bis und 269ter StPO und Art. 70bis und 70ter MStP) ad 10.3831 Mo. Schmid-Federer Barbara: BÜPF-Revision, vom 1.10.2010; Ziff. 2.2, 2.3, 2.6, 2.9 und 2.12 (ad Art. 6–18, 26 und 38, Art. 269bis und 269ter StPO und Art. 70bis und 70ter MStP) ad 10.3876 Mo. Eichenberger-Walther Corina: BÜPF-Revision, vom 1.10.2010; Ziff. 2.2, 2.3, 2.6, 2.9 und 2.12 (ad Art. 6–18, 26 und 38, Art. 269bis und 269ter StPO und Art. 70bis und 70ter MStP) ad 10.3877 Mo. (von Rotz Christoph) Schwander Pirmin: BÜPF-Revision, vom 1.10.2010; Ziff. 2.12 (ad Art. 269bis und 269ter StPO und Art. 70bis und 70ter MStP) ad 11.4042 Po. Kommission für Rechtsfragen NR: Überwachung mittels Trojanern (1), vom 11.11.2011; Ziff. 2.12 (ad Art. 269bis und 269ter StPO und Art. 70bis und 70ter MStP) ad 11.4043 Po. Kommission für Rechtsfragen NR: Überwachung mittels Trojanern (2), vom 11.11.2011; Ziff. 2.9 (ad Art. 38) ad 10.4210 Po. Recordon Luc: Kosten der Überwachung des Fernmeldeverkehrs im Rahmen eines Strafverfahrens, vom 23.12.2011.

17 Bernard Corboz, Les Infractions en droit suisse, Bd. II, Bern 2010, Art. 321ter StGB N 6.

18 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 14.

Absatz 1 Buchstabe a wird dahingehend geändert, dass die Erwähnung des Bundes- oder Kantonscharakters des Strafverfahrens aufgehoben wird. Diese Erwähnung wurde mit dem Inkrafttreten der StPO überflüssig, da diese sowohl für Verfahren des Bundes als auch der Kantone gilt und die Möglichkeit vorsieht, im Rahmen dieser Verfahren Überwachungen des Post- und Fernmeldeverkehrs durchzuführen.

Absatz 1 Buchstabe b weist sinngemäss die gleiche Formulierung auf wie im geltenden BÜPF.

Die Erwähnung der Rettung in *Absatz 1 Buchstabe c* des geltenden Gesetzes kann aufgehoben werden, da dieses Ziel die logische Folge der Absicht ist, nach einer vermissten Person zu suchen (Art. 35). Von *Absatz 1 Buchstabe c* ebenfalls erfasst wird die Suche nach Personen im Fall einer Katastrophe (siehe Erläuterungen zu Art. 35).

Nach *Absatz 1 Buchstabe d* ist das BÜPF neu anwendbar bei der Fahndung nach einer Person, gegen die durch ein rechtskräftiges und vollstreckbares Urteil eine Freiheitsstrafe oder eine freiheitsentziehende Massnahme verhängt wurde, unabhängig von der Art der begangenen Straftat (siehe Erläuterungen zu Art. 36).

Absatz 2 betrifft wie Absatz 3 des geltenden BÜPF die Auskünfte über den Zahlungsverkehr, der dem Postgesetz vom 17. Dezember 2010[19] (PG) untersteht. Der Verweis auf den Bundes- oder Kantonscharakter der Bestimmungen wird aufgehoben. Dieser Verweis wurde mit dem Inkrafttreten der StPO überflüssig, die sowohl für Verfahren des Bundes als auch der Kantone gilt und die Zeugnispflicht sowie in den Artikeln 284 und 285 die Auskunftspflicht gegenüber einer Behörde regelt. Bezüglich ihrer Tätigkeit im Zusammenhang mit dem Zahlungsverkehr ist die Post als «bankähnliches Institut» im Sinne von Artikel 284 StPO zu betrachten. Der in *Absatz 2* vorgenommene Verweis bezieht sich zum Beispiel auch auf die entsprechenden Bestimmungen im MStP.

Art. 2 Persönlicher Geltungsbereich

Artikel 2 legt wie Artikel 1 Absatz 2 des geltenden BÜPF den persönlichen Geltungsbereich des Gesetzes fest, d.h. die Personen, die diesem Gesetz unterstellt sind und denen daraus Pflichten erwachsen. Diese Personen werden im Entwurf und in der vorliegenden Botschaft allgemein als «Mitwirkungspflichtige» bezeichnet. Die verschiedenen (Überwachungs-)Pflichten jeder dieser Personenkategorien sind insbesondere in den Artikeln 19–30 des Entwurfs geregelt.

Bezüglich der Ausweitung des persönlichen Geltungsbereichs, die im VE-BÜPF gegenüber dem geltenden Gesetz vorgeschlagen wurde, gingen die Meinungen im Vernehmlassungsverfahren auseinander. Etliche Kantone und Organisationen im Bereich der Strafverfolgung unterstützten eine entsprechende Ausdehnung. Viele lehnten die geplante Ausweitung hingegen ab oder verlangten eine Umformulierung von Artikel 2 Absatz 1 Buchstabe b VE-BÜPF; dies gilt insbesondere für die Konsumentenschutzorganisationen und die Anbieterinnen von Fernmeldediensten. Es stellte sich die Frage, ob Artikel 2 Absatz 1 Buchstabe b VE-BÜPF verständlich formuliert sei oder ob er nicht zu weit gehe, insbesondere aufgrund seiner Tragweite und der wirtschaftlichen Auswirkungen auf die Betroffenen. Zudem wurde die Frage aufgeworfen, ob es angebracht sei, die Webhoster (Hosting-Provider) als Internet-

19 SR **783.0**

dienstanbieterinnen in den persönlichen Geltungsbereich des Gesetzes aufzunehmen. Siehe im Übrigen den Vernehmlassungsbericht[20].

Der persönliche Geltungsbereich ist im geltenden Recht tatsächlich zu wenig klar. Dies gilt vor allem für den Wortlaut von Artikel 2 Absatz 1 Buchstabe b VE-BÜPF. Dieser konnte so ausgelegt werden, dass diejenigen in den persönlichen Geltungsbereich des Gesetzes gefallen wären, die in irgendeiner Weise mit Kommunikationsdaten zu tun haben (zum Beispiel Unternehmen, die nur Lösungen im Bereich der Netzwerksicherheit anbieten). Dies ginge eindeutig zu weit, auch angesichts der Kosten, die den Betroffenen entstehen würden. Die unzureichende Klarheit wurde deshalb im Entwurf korrigiert.

Der Entwurf sieht vor, verschiedenen Kategorien von Personen (siehe die Erläuterungen zu den Buchstaben a–f), die durch ihre Tätigkeiten gekennzeichnet sind, verschiedene Pflichten zuzuweisen. Dabei muss jede dieser Tätigkeiten unabhängig von den anderen betrachtet werden. Je nach den Tätigkeiten, die ein Unternehmen ausübt, kann es ohne Weiteres mehreren dieser Kategorien angehören und somit entsprechend diesen Tätigkeiten unterschiedliche Überwachungspflichten haben (siehe Art. 19–30). Das BÜPF gilt für alle Personen, welche die Bedingungen einer der erwähnten Kategorien erfüllen. Dabei kann es sich um natürliche Personen oder sonstige staatliche oder andere Rechtssubjekte handeln, unabhängig davon, ob diese juristische Personen sind oder nicht.

Der persönliche Geltungsbereich des BÜPF wird somit gegenüber dem geltenden Recht präzisiert und geändert. Dort sind nur die Anbieterinnen von Post- oder Fernmeldediensten, zu denen auch die Internetzugangsanbieterinnen gehören, sowie die Betreiberinnen von internen Fernmeldenetzen und Hauszentralen aufgeführt. Daneben können jedoch weitere Personen zu bestimmten Zeitpunkten Daten im Zusammenhang mit dem Post- oder Fernmeldeverkehr besitzen, welche die Strafverfolgungsbehörden im Rahmen der Kriminalitätsbekämpfung von Interesse sein könnten. Somit ist es berechtigt, dass das BÜPF diesen Personen Pflichten im Bereich der Überwachung dieses Verkehrs überträgt. Dies gilt beispielsweise für jene Internetdienstanbieterinnen, die als Webhoster (Hosting-Provider) tätig sind (siehe die Erläuterungen zu Bst. c).

Der persönliche Geltungsbereich des BÜPF wird gegenüber dem geltenden Gesetz auch dahingehend geändert, dass die Anbieterinnen von Post- oder Fernmeldediensten neu nicht mehr konzessions- oder meldepflichtig sein müssen, um in diesen Geltungsbereich zu fallen (siehe die Erläuterungen zu den Bst. a und b)[21].

Buchstabe a erfasst nicht nur Die Schweizerische Post als Anbieterin von Postdiensten, sondern auch alle anderen Akteure im Postmarkt, die solche Dienste anbieten. Im Gegensatz zur Regelung im geltenden BÜPF sieht der Entwurf nicht mehr vor, für die Frage der Unterstellung einer Anbieterin von Postdiensten unter das BÜPF auf die Tatsache abzustellen, dass sie konzessions- oder meldepflichtig ist. Dies bedeutet insbesondere, dass auch Anbieterinnen in den persönlichen Geltungsbereich des Gesetzes fallen, die nicht der ordentlichen Meldepflicht nach Artikel 3 der Postverordnung vom 29. August 2012[22] unterstehen. In diesen Geltungsbereich fallen deshalb zum Beispiel auch die Anbieterinnen von Kurierdiensten und Eil-

20 www.admin.ch/ch/d/gg/pc/documents/1719/Bericht_V_Ueberwachung_des_Post-und_Fernmeldeverkehrs.pdf
21 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 1 BÜPF N 24.
22 SR **783.01**

postdiensten. Hingegen werden die Anbieterinnen von Postdiensten, die Bankdienstleistungen erbringen, für diese Tätigkeit hier nicht erfasst (siehe auch die Erläuterungen zu Art. 1 Abs. 2).

Buchstabe b erfasst die zentralen Akteure im Bereich der Überwachung des Fernmeldeverkehrs: die Anbieterinnen von Fernmeldediensten. In der Fernmeldegesetzgebung ist definiert, was eine Anbieterin von Fernmeldediensten im Sinne des BÜPF ist. Massgebend sind Artikel 3 Buchstaben a–c, namentlich Buchstabe b, FMG sowie Artikel 2 der Verordnung vom 9. März 2007[23] über Fernmeldedienste (FDV). Wer nach dieser Gesetzgebung als Anbieterin von Fernmeldediensten gilt, ist es auch gemäss dem BÜPF. Zusammenfassend verpflichten sich die Fernmeldedienstanbieterinnen, im Auftrag von Dritten, d.h. für die Öffentlichkeit, Informationen (im Sinne von Artikel 3 Buchstabe a FMG) fernmeldetechnisch (im Sinne von Art. 3 Bst. c FMG) selber zu befördern oder zu übertragen. Die Buchstabe c unterstehenden Personen wie die Webhoster (Hosting-Provider) sind keine Fernmeldedienstanbieterinnen, da sie keine Daten übertragen oder befördern, schon gar nicht selbst (siehe die Erläuterungen zu Bst. c). Dasselbe gilt für die Personen, die unter Buchstabe e fallen, wie zum Beispiel Internet- oder Cybercafés und Hotels, da sie nicht selbst Daten übertragen (siehe die Erläuterungen zu Buchstabe e). Die gleiche Situation besteht bei den Personen, die von Buchstabe d erfasst werden, da sie keine Daten für Dritte, d.h. für die Öffentlichkeit, übertragen (siehe die Erläuterungen zu Bst. d). Anbieterinnen von Fernmeldediensten sind zum Beispiel die grossen Unternehmen wie Swisscom, Orange, Sunrise und Cablecom, die im Schweizer Markt tätig sind. Sie ermöglichen den Teilnehmerinnen und Teilnehmern, mit einem Festnetz- oder Mobiltelefon zu telefonieren oder auf das Internet zuzugreifen. Die Internetzugangsanbieterinnen gelten als Fernmeldedienstanbieterinnen im Sinne der Fernmeldegesetzgebung und folglich auch im Sinne des BÜPF; dies gilt unabhängig davon, ob sie daneben eine weitere Tätigkeit wie zum Beispiel einen Telefondienst betreiben. Keine Fernmeldedienstanbieterinnen sind hingegen die anderen Internetanbieterinnen wie zum Beispiel die Internetdienstanbieterinnen, insbesondere die Webhoster (Hosting-Provider). Diese werden allenfalls von Buchstabe c erfasst (siehe im Übrigen die Erläuterungen zu Bst. c).

Im Gegensatz zum geltenden BÜPF sieht *Buchstabe b* nicht mehr vor, dass nur die konzessions- oder meldepflichtigen Fernmeldedienstanbieterinnen dem persönlichen Geltungsbereich des Gesetzes unterstehen. Theoretisch ist es somit möglich, dass eine Fernmeldedienstanbieterin von den Pflichten ausgenommen ist, die sich nach den Artikeln 4 Absatz 2 FMG und 3 FDV aus der Fernmeldegesetzgebung ableiten, aber dennoch Pflichten nach der Gesetzgebung im Bereich der Überwachung des Post- und Fernmeldeverkehrs untersteht, wobei auch diese Gesetzgebung solche Ausnahmen vorsehen kann (siehe die Erläuterungen zu Art. 26 Abs. 6).

Buchstabe c erfasst Personen, die weder Internetzugangsanbieterinnen noch Fernmeldedienstanbieterinnen im Sinne des Gesetzes sind (siehe die Erläuterungen zu Bst. b), jedoch insbesondere im Bereich des Internetverkehrs ebenfalls eine Rolle spielen, indem sie Dienste bereitstellen, die nur in Verbindung mit der Tätigkeit einer Fernmeldedienstanbieterin, insbesondere einer Internetzugangsanbieterin, angeboten werden können. Diese Personen sind keine Fernmeldedienstanbieterinnen, da sie keine Daten übertragen oder befördern, schon gar nicht selbst. Ohne Inanspruchnahme einer Fernmeldedienstanbieterin, die Daten überträgt, können

23 SR **784.101.1**

diese Personen, die Internetdienstanbieterinnen sind, ihre Dienste nicht anbieten. Sie werden deshalb im Folgenden als «Anbieterinnen abgeleiteter Kommunikationsdienste» bezeichnet.

Buchstabe c erfasst die Anbieterinnen von zwei Arten von Internetdiensten: Die einen ermöglichen eine Einwegkommunikation, die das Hochladen von Dokumenten gestattet (zum Beispiel Google docs oder Microsofts office.live.com), die anderen eine Mehrwegkommunikation, welche die Kommunikation zwischen Nutzerinnen und Nutzern erlaubt (zum Beispiel Facebook). Dabei ist nicht von Belang, ob die Kommunikation synchron oder asynchron erfolgt. Unter diesen Buchstaben fallen zum Beispiel Anbieterinnen von Speicherplatz für E-Mails, die verschiedenen Arten von Webhostern (Hosting-Provider), die z.B. das Hosting von Anwendungen oder E-Mail-Diensten (z.B. .gmx), Hosting in Form von «server colocation» oder «server housing» mit Zugriff (z.B. Green.ch und Colt), «facility management»-Hosting ohne Kommunikationsdienste (reine Colocation) oder Cloud-Services anbieten; ebenfalls unter diesen Buchstaben fallen Chat-Plattformen, Plattformen für den Dokumentenaustausch sowie Anbieterinnen von Internettelefoniediensten des Typs Peer-to-Peer (z.B. Skype Peer-to-Peer). Diesbezüglich ist klarzustellen, dass zum Beispiel ein Unternehmen, das ein Verschlüsselungsprodukt anbietet, nicht die Kommunikation im Sinne von *Buchstabe c* «ermöglicht», sondern sie höchstens erleichtert. Daher wird es von dieser Bestimmung und somit vom persönlichen Geltungsbereich des BÜPF nicht erfasst. Es ist weiter zu beachten, dass ein Unternehmen, zum Beispiel Swisscom, aufgrund seiner Tätigkeiten zugleich als Fernmeldedienstanbieterin (Buchstabe b) gilt und unter Buchstabe c fallen kann, weil es neben seiner Tätigkeit als Internetzugangsvermittler auch als E-Mail-Provider oder Webhoster (Hosting-Provider) in Erscheinung tritt. Gegebenenfalls können ihm aufgrund dieser verschiedenen Tätigkeiten unterschiedliche Überwachungspflichten zukommen (siehe die Art. 26 und 27).

Wie bereits aus den oben angeführten Beispielen von Unternehmen hervorgeht, sollte jedoch in Bezug auf die Fernmeldeüberwachung keine allzu grosse Hoffnung in die Tatsache gesetzt werden, dass die von *Buchstabe c* erfassten Personen in den persönlichen Geltungsbereich aufgenommen werden, da viele bedeutende Anbieterinnen der entsprechenden Internetdienste ihren Sitz und ihre Infrastruktur im Ausland haben. Ein gutes Beispiel dafür sind gewisse im Ausland eröffneten E-Mail-Konten – also Dienste, die an sich technisch kontrollierbar sind – die von Personen mit Wohnsitz in der Schweiz eröffnet werden. Es wäre somit unrealistisch und problematisch, generell vorzusehen, dass die schweizerischen Behörden ohne Weiteres auf die betreffenden Daten zugreifen können, da dies gegen den Grundsatz der Territorialität der Gesetze verstossen würde. Eine solche Regelung besteht im geltenden Recht nicht. Zur Herausgabepflicht von (Rand-)Daten der Anbieterinnen abgeleiteter Kommunikationsdienste vgl. die Erläuterungen zu Artikel 27 Absatz 2.

Die von *Buchstabe d* erfassten Personen sind keine Fernmeldedienstanbieterinnen (siehe die Erläuterungen zu Bst. b). Sie bieten die Dienste nicht Dritten an, d.h. der Öffentlichkeit, sondern nur einem beschränkten Kreis von Personen mit einer besonderen Eigenschaft; ihre Netze sind also nicht für alle zugänglich. Darunter fällt zum Beispiel ein Unternehmen, das seinen Mitarbeiterinnen und Mitarbeitern ein Fernmeldenetz für die Kommunikation untereinander zur Verfügung stellt oder eine öffentliche Einrichtung, die ihre Angestellten über ein solches Netz miteinander kommunizieren lässt (siehe auch Art. 2 FDV). Erfasst werden die gleichen Personen wie in Artikel 1 Absatz 4 des geltenden BÜPF. Allerdings sind nur noch die Betrei-

berinnen von internen Fernmeldenetzen erwähnt, während die Betreiber von Hauszentralen nicht mehr aufgeführt sind, da der Begriff der Hauszentrale, der das Bestehen eines Netzes voraussetzt, im Begriff des internen Fernmeldenetzes enthalten ist. Siehe auch die Erläuterungen zu Artikel 28.

Buchstabe e bezieht sich auf Personen, die ihren Zugang Dritten zur Verfügung stellen. Dabei kann es sich um Hotels, Restaurants, Cafés, Internet- oder Cybercafés, Spitäler, Schulen usw. handeln, die ihren Internetzugang (WLAN, kabelgebunden oder in anderer Form) Dritten verfügbar machen, insbesondere ihrer Kundschaft, ihren Patientinnen und Patienten, ihren Studierenden usw. Unter diesen Buchstaben kann auch eine Privatperson fallen, deren Zugang Dritten absichtlich oder unabsichtlich offensteht. Die Aufnahme dieser Personen in den persönlichen Geltungsbereich des Gesetzes ergibt sich insbesondere aus den Forderungen, die in der Motion 07.3627 Glanzmann-Hunkeler gestellt werden; zurzeit werden diese Personen im persönlichen Geltungsbereich nicht genannt. Sie sind keine Fernmeldedienstanbieterinnen, da sie nicht selbst Informationen für Dritte übertragen; diese Funktion kommt anderen Personen zu: den Anbieterinnen von Fernmeldediensten wie zum Beispiel Swisscom, Orange, Sunrise und Cablecom (siehe die Erläuterungen zu Bst. b). Für den Zusammenhang zwischen den Pflichten der Personen, die unter Buchstabe e fallen, und der Motion 07.3627 Glanzmann-Hunkeler, siehe die Erläuterungen zu Artikel 29.

Buchstabe f ist relativ offen formuliert, damit der Entwicklung der Technik Rechnung getragen werden kann. Er betrifft nicht nur den Bereich der Mobiltelefonie, sondern auch die Festnetztelefonie und den Internetbereich, und erfasst somit heute vor allem die Wiederverkäufer von Mitteln wie Prepaid-SIM-Karten und Prepaid-Wireless-Karten. Nicht betroffen sind die Wiederverkäufer von 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»). Die von *Buchstabe f* erfassten Wiederverkäufer (zum Beispiel Interdiscount, Media Markt und Mobilezone) sind keine Anbieterinnen von Fernmeldediensten (siehe die Erläuterungen zu Buchstabe b), sondern Wiederverkäufer von Geräten dieser Anbieterinnen (z.B. Swisscom, Orange und Sunrise). Die Aufnahme der Wiederverkäufer von Wireless-Prepaid-Karten in den persönlichen Geltungsbereich des Gesetzes ergibt sich insbesondere aus den Forderungen, die in der Motion 07.3627 Glanzmann-Hunkeler gestellt werden. Die Personen, die unter *Buchstabe f* fallen, unterstehen heute nicht dem persönlichen Geltungsbereich. Mit dieser Bestimmung soll zudem eine Lücke geschlossen werden, die in Bezug auf die Pflicht der Fernmeldedienstanbieterinnen zur Aufzeichnung der Daten ihrer Kundinnen und Kunden besteht, denen sie Prepaid-SIM-Karten verkaufen (siehe die Erläuterungen zu Art. 30). Für die Pflichten der Wiederverkäufer von Prepaid-Wireless-Karten, siehe die Erläuterungen zu Artikel 30.

Art. 3 Überwachungsdienst

Artikel 3 entspricht Artikel 2 des geltenden BÜPF und ergänzt diesen.

Nach *Absatz 1* ist der Dienst die Schnittstelle zwischen den Strafverfolgungsbehörden, die Überwachungen anordnen, und den Personen, die unter den persönlichen Geltungsbereich des Gesetzes fallen (insbesondere den Anbieterinnen von Fernmeldediensten) und die angeordneten Überwachungen durchführen. Dabei ist zu präzisieren, dass der Dienst diese Rolle ausschliesslich für Massnahmen zur Überwa-

chung des Post- und Fernmeldeverkehrs nach Artikel 269 StPO spielt, also in Zusammenhang mit der klassischen Überwachung. Beim Einsatz von technischen Überwachungssystemen wie IMSI-Catchern und GovWare hingegen kommt ihm keine besondere Aufgabe zu, was heisst, dass er dafür auch keine Überwachungsanordnung erhalten muss (für Einzelheiten, siehe Erläuterungen zu Art. 269bis und 269ter StPO).

In *Absatz 2* wird Artikel 2 Absatz 2 des geltenden BÜPF übernommen. Die Unabhängigkeit des Dienstes betrifft jedoch das Verhältnis zum EJPD und zum Bundesrat und nicht dasjenige zu den Strafverfolgungsbehörden. Gegenüber den Strafverfolgungsbehörden ist der Dienst im hierarchischen Sinn ohnehin unabhängig, das heisst, es besteht kein Weisungsrecht gegenüber dem Dienst und kein Recht, im Bereich der Aufgaben des Dienstes an dessen Stelle zu handeln. Der Dienst ist jedoch an die vollstreckbaren Überwachungsanordnungen der Strafverfolgungsbehörden gebunden. Die Unabhängigkeit gegenüber EJPD und Bundesrat ist wichtig, um diese Vollzugsfunktion des Dienstes sicherzustellen: Er müsste zwei Herren dienen, wenn er gleichzeitig an eine gerichtlich genehmigte Anordnung und an allfällige Weisungen des EJPD gebunden wäre. Als politische Behörde käme das EJPD zudem in eine unangenehme Lage, wenn es als Aufsichtsbehörde die Verantwortung für Handlungen des Dienstes übernehmen müsste, die durch gerichtlich genehmigte Anordnungen vorgegeben sind. Hinsichtlich des Personalrechts bleibt darauf hinzuweisen, dass das Bundespersonalgesetz vom 24. März 2000[24] und die Bundespersonalverordnung vom 3. Juli 2001[25] auf Mitarbeitende des Dienstes Anwendung findet.

Die Zusammenarbeit nach *Absatz 3* muss gegenseitig sein. Die in diesem Absatz genannten Behörden, insbesondere das BAKOM und die Strafverfolgungsbehörden, sind gehalten, den Dienst im Rahmen des Gesetzes bei der Erfüllung seiner Aufgaben zu unterstützen. *Absatz 3* erteilt den Partnerbehörden des Dienstes keine Kontrollaufgabe hinsichtlich der Gesetzgebung im Bereich der Überwachung des Post- und Fernmeldeverkehrs. Die administrative Aufsicht ist in Artikel 41 geregelt.

Art. 4 Bearbeitung von Personendaten

Artikel 4 lehnt sich an den geltenden Artikel 7 Absatz 1 VÜPF an. Er betrifft insbesondere auch die Polizei; dies gilt nicht nur für den Fall, dass sie in eigener Regie handelt, sondern auch dann, wenn sie auf Anordnung der Staatsanwaltschaft handelt. Die Einzelheiten im Zusammenhang mit den Modalitäten der Bearbeitung sind weiterhin in der oben erwähnten Verordnung geregelt.

Art. 5 Beratendes Organ

Da die verschiedenen Akteure im Bereich der Überwachung des Post- und Fernmeldeverkehrs entgegenstehende Interessen verfolgen können, ist es äusserst wichtig, dass sie in einem beratenden Organ zusammenarbeiten, um die reibungslose Durchführung der Überwachungen und die ständige Weiterentwicklung in diesem Bereich zu fördern. Dies hat die Erfahrung gezeigt. Eine Zusammenarbeit besteht schon heute auf informeller Grundlage, ohne dass dafür eine gesetzliche Grundlage bestand. Die neue Bestimmung unterstreicht jedoch die Wichtigkeit der Zusammen-

24 SR **172.220.1**
25 SR **172.220.111.3**

arbeit und bestärkt die Beteiligten, sich in einem formell konstituierten Organ zu engagieren. Zur Erreichung des erwähnten Ziels ist es nicht notwendig, dem Organ Entscheidungsbefugnisse zu übertragen. Es genügt, ihm eine beratende Rolle zuzuweisen, die es jedoch aktiv ausüben kann, indem es von sich aus Empfehlungen abgibt. *Artikel 5* ermöglicht es dem EJPD, diese Zusammenarbeit formell festzulegen.

Absatz 1 bildet die Rechtsgrundlage für eine formelle Zusammenarbeit zwischen den verschiedenen Akteuren im Bereich der Überwachung des Post- und Fernmeldeverkehrs. Er gibt dem EJPD die Möglichkeit, zu diesem Zweck ein beratendes Organ einzusetzen, dem Vertreterinnen und Vertreter dieser Akteure angehören.

Absatz 2 steckt einen allgemeinen Rahmen für die Tätigkeiten des beratenden Organs vor und enthält die Ziele, die durch dieses angestrebt werden.

Absatz 3 überträgt dem EJPD die Aufgabe, Detailbestimmungen zu erlassen und darin die Zusammensetzung und die Arbeitsweise des beratenden Organs zu regeln, das es nach Absatz 1 einsetzen kann.

Das EJPD legt fest, welche Organisationen im beratenden Organ mitwirken können, und wer bestimmen kann, von welchen natürlichen Personen diese Organisationen vertreten werden. Da es primär um den Erfahrungsaustausch zwischen den beteiligten Behörden und Unternehmen geht, sollte sich die Zusammensetzung des Organs auch ad hoc ergeben können, je nachdem, welches Spezialwissen (technischer oder administrativer Art) gefragt ist. In diesem Sinne lässt sich beispielsweise vorsehen, dass jede Organisation entsprechend den behandelten Themen eine Person aufgrund ihrer Kompetenzen entsenden kann. Zu klären ist zudem die Frage, ob noch weitere Personen eingeladen werden können, im beratenden Organ mitzuwirken, und welche Kompetenzen ihnen diesfalls zukommen. Weiter wird sich das EJPD bestimmen müssen, wer mit welchen Kompetenzen den Vorsitz und das Sekretariat des beratenden Organs übernimmt, wie die Beschlüsse innerhalb des Organs gefasst werden, wie die Stellungnahmen und Empfehlungen des beratenden Organs veröffentlicht werden und welche Informationen allenfalls dem Amtsgeheimnis unterstellt werden müssen. Die Teilnehmerinnen und Teilnehmer werden nicht vom Bund entschädigt, sondern von den Organisationen, die sie vertreten.

2.2 2. Abschnitt: Informatiksystem zur Verarbeitung von Daten im Rahmen der Überwachung des Fernmeldeverkehrs

Die Artikel 6–14 regeln die Arbeitsweise des neuen, vom Dienst betriebenen Informatiksystems zur Verarbeitung (bzw. Bearbeitung) der Daten über die Fernmeldeüberwachung, d.h. des «Interception System Schweiz» (ISS). Das System wird insbesondere die Daten enthalten, die durch die Überwachung des Fernmeldeverkehrs nach Artikel 269 StPO gesammelt werden, also die Daten aus der klassischen Überwachung. Die Daten aus Überwachungen mittels technischer Einrichtungen wie IMSI-Catchern oder GovWare hingegen wird es nicht umfassen. Das ISS soll somit ausschliesslich Daten empfangen, die mit der Tätigkeit des Dienstes zusammenhängen. Die durch IMSI-Catcher oder GovWare gesammelten Daten gehören nicht dazu, und das ISS ist kein Polizeisystem (für Einzelheiten, siehe Erläuterungen zu Art. 269bis und 269ter StPO).

Gemäss seiner Antwort auf die Ziffer 3 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision) hat sich der Bundesrat mit der Frage befasst, ob es angebracht ist, dieses System dem Bundesgesetz vom 13. Juni 2008[26] über die polizeilichen Informationssysteme des Bundes (BPI) zu unterstellen. Dabei gelangte er zum Schluss, dass dies nicht der Fall ist. Das BPI soll gemäss dem Wortlaut seiner Artikel 1 und 2 nur auf die von fedpol betriebenen Informationssysteme anwendbar sein, während das System zur Verarbeitung von im Rahmen einer Überwachung des Fernmeldeverkehrs gesammelten Daten allein vom Dienst betrieben wird. Dafür spricht auch, dass der Dienst keine Strafbehörde ist, insbesondere keine Strafverfolgungsbehörde.

Die zentrale Langzeitaufbewahrung der Daten und die Artikel 6–13 VE-BÜPF, namentlich die Artikel 9–11, wurden im Rahmen des Vernehmlassungsverfahrens unterschiedlich aufgenommen. Mehrere Kantone, Organisationen aus dem Bereich der Strafverfolgung sowie die Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) unterstützten die zentrale Aufbewahrung grundsätzlich, verlangten jedoch Anpassungen nach dem Vorbild des bisherigen Systems. Andere, insbesondere die Kantone, forderten, dass nur die durch Internetüberwachungen gesammelten Daten angesichts ihres Umfangs zentral aufbewahrt und dass die anderen Daten weiterhin per Post auf Datenträgern zugestellt werden sollen. Eine grössere Zahl von Kantonen und Organisationen im Bereich der Strafverfolgung zeigte sich kritischer. Einige erachteten die vorgesehene Regelung als äusserst kompliziert und zogen die Vereinbarkeit mit der StPO in Zweifel. Andere stellten sich gegen die zentrale Aufbewahrung dieser Daten beim Dienst und lehnten den Online-Zugriff auf diese Daten, auch für die beschuldigte Person und ihren Rechtsbeistand, aus sicherheitstechnischen Gründen ab. Sie würden es vorziehen, diese Daten auf Datenträgern zu erhalten. Eine weitere Gruppe von Vernehmlassungsteilnehmern kritisierte beide erwähnten Punkte.

Nach Prüfung der Frage beantragt der Bundesrat letztlich, die zentrale Langzeitaufbewahrung der durch die Fernmeldeüberwachung gesammelten Daten im vom Dienst betriebenen System vorzusehen. Dies wird insbesondere vom Dienst und von bestimmten Vertretern der Strafverfolgungsbehörden unterstützt. Diese Aufbewahrung gilt für alle Daten, die aus Überwachungen des Fernmeldeverkehrs hervorgehen, für die Daten aus traditionellen Telefonüberwachungen sowie für Daten, die aus Internetüberwachungen stammen. Mit dieser Botschaft werden jedoch zweckmässigere, einfachere und praktikablere Bestimmungen vorgeschlagen als im VE-BÜPF (siehe die Erläuterungen zu Art. 9–11).

Die vorgesehene Betriebsweise ersetzt die bisherige, bei welcher der Dienst alle gesammelten Daten auf Datenträgern per Post an die (Strafverfolgungs-)Behörden übermittelt. Sobald diese dem Dienst den Empfang bestätigt haben, löscht er nach der heute geltenden Regelung die Daten in seinem System. Wie alle anderen Beweismittel eines Verfahrens werden die Daten, die allenfalls durch die Polizei oder eine andere Stelle transkribiert werden, in den Gerichtsakten aufbewahrt.

Bei der nun vorgeschlagenen Betriebsweise können die (Strafverfolgungs-)Behörden die durch die Überwachung des Fernmeldeverkehrs gesammelten Daten zu den Verfahren, mit denen sie befasst sind, über einen Online-Zugriff auf das Verarbei-

26 SR **361**

tungssystem abrufen, das vom Dienst betrieben wird. Auch die Parteien, einschliesslich der beschuldigten Person und ihres Anwalts, können online auf diese Daten zugreifen. Dazu wird ihnen bei der Behörde, die mit dem Verfahren befasst ist, ein Endgerät für den Zugriff zur Verfügung gestellt. Auf Anfrage und unter bestimmten Bedingungen können jedoch die Daten, die bei Überwachungen des Fernmeldeverkehrs gesammelt werden, wie bisher auf mobilen Datenträgern übermittelt werden. Zu diesem Zweck werden die Daten verschlüsselt. Es ist nicht wünschenswert, dass ausländische Behörden im Rahmen eines internationalen Rechtshilfeverfahrens Zugang zum Verarbeitungssystem des Dienstes erhalten, um diese Daten abzurufen.

Die Aufhebung der bestehenden Regelung und der Übergang zur zentralen (Langzeit-)Aufbewahrung der Daten im Verarbeitungssystem des Dienstes stiessen in der Vernehmlassung auf Widerstand. Dennoch spricht vor allem ein Argument für diese Lösung: Die Daten, die im Rahmen der einzelnen Überwachungen zusammengetragen werden, vor allem jene aus Internetüberwachungen, werden immer umfangreicher. Daher lassen sie sich immer schlechter per Post auf Datenträgern an die Behörden übermitteln. Zudem wird es vor allem aus Platzgründen immer schwieriger, diese Datenträger zu lagern und zu verwalten. Dies gilt zumindest in den grössten Kantonen. Angesichts der künftigen technischen Entwicklungen wird sich diese Tendenz in den kommenden Jahren noch verstärken. Mit der vorgeschlagenen Änderung kann dieses Problem gelöst werden. Gleichzeitig lässt sich die Datensicherheit verbessern, indem bestimmte Risiken ausgeschaltet werden, die mit dem heute geltenden System des Postversands der Daten verbunden sind (zum Beispiel Verlust, Diebstahl und Kopieren der Datenträger). Ausserdem wird eine bessere Zusammenarbeit zwischen den verschiedenen Strafverfolgungsbehörden ermöglicht, die mit dem Verfahren, aus dem die Kommunikationsdaten stammen, befasst sind. Gemäss der vorgeschlagenen Regelung muss der Dienst unter Berücksichtigung der technischen Entwicklung zentral sicherstellen, dass die Daten im Verarbeitungssystem, das er betreibt, langfristig lesbar bleiben. Dies bietet ausserdem den Vorteil, dass diese Aufgabe nicht von jedem Kanton einzeln wahrgenommen werden muss. Diese Änderung erleichtert zudem den Einsatz der erforderlichen Programme für die Auswertung der Daten, da nicht mehr das Risiko besteht, dass das Verarbeitungssystem des Dienstes und die dezentral von den Kantonen betriebenen Systeme nicht kompatibel sind.

Die zentrale Langzeitaufbewahrung der durch die Fernmeldeüberwachung gesammelten Daten im Verarbeitungssystem des Dienstes verursacht Mehrkosten für den Bund. Hingegen dürften für die Kantone geringere Ausrüstungskosten anfallen. Die Mehrkosten, die für den Bund aufgrund der längeren Fristen für die Aufbewahrung der Daten beim Dienst anfallen, können sich auf die Gebühren auswirken, die von den Strafverfolgungsbehörden, insbesondere von jenen der Kantone, zu entrichten sind (Art. 38 Abs. 3). Da diese Änderung zu erheblichen Verbesserungen führen wird und die mit den Überwachungen verbundenen Kosten im Vergleich zur Gesamtheit der Strafverfolgungskosten sehr gering sind, lassen sich die zu erwartenden Mehrkosten jedoch vertreten. Diese Kosten sind von jenen zu unterscheiden, die mit dem Erwerb des ISS verbunden sind. Siehe auch unten, Ziffer 3.1.

Art. 6 Grundsatz

Artikel 6 lehnt sich an Artikel 8 Absatz 1 der geltenden VÜPF an. Er ermächtigt den Dienst, ein solches System zu betreiben. Das System kann aus mehreren Teilsystemen bestehen und auf verschiedenen Servern betrieben werden. In Artikel 8 wird

festgelegt, welche Daten das vom Dienst betriebene Verarbeitungssystem enthält. Es enthält keine Daten aus der Überwachung des Postverkehrs, da diese der anordnenden Behörde gemäss Artikel 19 direkt übermittelt werden. Das System muss angemessen abgesichert werden (siehe die Erläuterungen zu Art. 12).

Art. 7 Zweck des Verarbeitungssystems

Das in *Buchstabe a* genannte Ziel ist der Hauptzweck des ISS. Abgesehen vom Abrufverfahren stimmt es mit dem Zweck des aktuellen Systems zur Verarbeitung der im Rahmen der Fernmeldeüberwachung gesammelten Daten überein. Betroffen sind die Daten zum Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs. Siehe im Übrigen die Erläuterungen zu Artikel 8 Buchstaben a und b. In Artikel 9 ist festgelegt, wer Zugang zu diesen Daten hat und in welchen Fällen dieser Zugang nicht über ein Abrufverfahren erfolgt. Siehe im Übrigen die einleitenden Erläuterungen zu Ziffer 2.2.

Der Gegenstand von *Buchstabe b* ist die Speicherung von Daten über einen längeren Zeitraum. Siehe im Übrigen die einleitenden Erläuterungen zu Ziffer 2.2.

Buchstabe c betrifft die Auskünfte nach den Artikeln 15, 21 und 22. Artikel 23 regelt die Modalitäten betreffend diese Auskünfte, namentlich in Bezug auf den Zugang. Für weitere Einzelheiten, siehe die Erläuterungen zu den Artikeln 15 und 21–23.

Die Daten, welche nach *Buchstabe d* im Informatiksystem des Dienstes verarbeitet werden können, entsprechen den Daten nach Artikel 8. Die Bearbeitungsfunktionen stehen der beschuldigten Person (und deren Verteidigung) nicht zur Verfügung. Die beschuldigte Person erhält nach Massgabe der strafprozessualen Regeln Zugang zu ihren Daten (siehe die Erläuterungen zu Art. 9 Abs. 1). Die Auswertung der Überwachungsdaten durch die Strafverfolgungsbehörden erfolgt in den entsprechenden Informationssystemen des polizeilichen Informationssystem-Verbundes des Bundesamtes für Polizei (siehe die Erläuterungen zu Art. 14).

Buchstabe e betrifft die Ausführung der Anordnungen zur Überwachung des Fernmeldeverkehrs und die Kontrolle dieser Ausführung (z.B. Controlling, Auftragserfassung, Auftragserteilung und Verwaltung).

Art. 8 Inhalt des Verarbeitungssystems

Die in *Artikel 8 Buchstaben a und b* erwähnten Daten entsprechen jenen, die im Rahmen einer Überwachung des Fernmeldeverkehrs beschafft werden dürfen. Für Einzelheiten siehe die Erläuterungen zu Artikel 26 Absatz 1. Zu den *Buchstaben c und d* siehe die Erläuterungen zu Artikel 7 Buchstaben c und e.

Art. 9 Zugriff auf das Verarbeitungssystem

Artikel 9 VE-BÜPF wurde im Vernehmlassungsverfahren von verschiedener Seite kritisiert. Insbesondere wurde bemängelt, die vorgeschlagene Regelung sei zu kompliziert, pannenanfällig und berücksichtige die derzeitigen Möglichkeiten nicht, Verfahren abzutreten, zu vereinigen oder zu trennen; darüber hinaus sei die vorgeschlagene Regelung unnötig. Der Bundesrat erachtet diese Kritik grösstenteils als berechtigt. Deshalb wird im vorliegenden Entwurf eine zweckmässigere, einfachere und praktikablere Lösung für die Behörden, vor allem für die Strafverfolgungsbe-

hörden, vorgeschlagen. Gegenüber der Regelung, die in Artikel 9 VE-BÜPF vorgesehen war, verringert sich damit auch der administrative Aufwand für den Dienst.

Die Bestimmung in *Absatz 1* entspricht grundsätzlich der heutigen Situation. Der Dienst hat die Online-Zugriffsberechtigungen auf das Verarbeitungssystem zu gewähren. Die Behörde, welche die Überwachung anordnete oder die Behörde, der später die Verfahrensleitung obliegt – kurz gesagt: die mit dem Verfahren befasste Behörde –, hat Zugriff auf die im Verarbeitungssystem gespeicherten Daten. Der in *Absatz 1* vorgeschlagene Wortlaut erlaubt folglich auch derjenigen Behörde, welche ein Dossier übernommen hat, auf die entsprechenden Daten zuzugreifen, selbst wenn sie die Überwachung nicht selber angeordnet hat. In diesem Zusammenhang ist insbesondere an eine Behörde zu denken, die sich nach einer Verfahrensvereinigung oder nach einer Beschwerde mit einem solchen Dossier zu befassen hat. Die Behörde nach *Absatz 1* ist Inhaberin der Datensammlung (siehe Art. 13). Gemäss dem Grundsatz der Verhältnismässigkeit kann eine Behörde im Sinne von *Absatz 1* nicht alle bei sämtlichen Überwachungen gesammelten Daten abrufen, die im Verarbeitungssystem enthalten sind. Sie erhält nur Zugang zu jenen Daten, die durch die jeweilige Überwachung gesammelt wurden. Nach der vorgeschlagenen Regelung können mit Bewilligung der Staatsanwaltschaft, die für das Verfahren zuständig ist, zum Beispiel auch an einem Fall arbeitende Polizisten die durch eine Überwachung gesammelten Daten online abrufen. Nur schweizerische Behörden erhalten Zugang zum Verarbeitungssystem des Dienstes, um solche Daten abzurufen. Es ist nicht wünschenswert, dass ausländische Behörden, insbesondere im Rahmen eines internationalen Rechtshilfeverfahrens, darauf zugreifen können (siehe Abs. 4). Die Parteien, einschliesslich der beschuldigten Person und ihres Anwalts, können die Fernmeldedaten im Zusammenhang mit dem Verfahren, das sie betrifft, im Rahmen ihres Anspruchs auf rechtliches Gehör (Art. 29 Abs. 2 der Bundesverfassung[27] [BV]) online abrufen. Dazu wird ihnen bei der Behörde, die mit dem Verfahren befasst ist, ein Endgerät für den Zugriff zur Verfügung gestellt.

Mit der in *Absatz 2* vorgesehenen Regelung lässt sich verhindern, dass Behörden nach Absatz 1 und die von ihnen bezeichneten Personen ausserhalb von Verfahren, mit denen sie befasst sind, auf Daten zugreifen, die sie nicht mehr benötigen. Eine Behörde kann während zahlreicher Jahre mit einem Verfahren befasst sein. Es ist aber nicht unbedingt notwendig, dass der Zugang zu den Daten während der ganzen Zeitdauer aktiv gewährleistet ist. Deshalb kann es sinnvoll sein, nach Ablauf einer bestimmten Zeitdauer einen Deaktivierungsmechanismus und eine Reaktivierung des betreffenden Online-Zuganges vorzusehen. Der Bundesrat erlässt die entsprechenden Vorschriften im Rahmen von Artikel 12 Absatz 2.

Die in *Absatz 3* vorgesehene Informationspflicht soll einerseits die Einhaltung von Absatz 2 sicherstellen. Andererseits soll sie dem Dienst die notwendigen Informationen für den Entscheid liefern, ob er einer anderen Behörde als der, welcher er ursprünglich den Online-Zugriff gewährt hat, ebenfalls nach Absatz 1 den Zugriff auf die Daten gewähren muss (siehe auch die Erläuterungen zu Abs. 1). Der Bundesrat kann die Modalitäten der Informationspflicht nach *Absatz 3* festlegen.

27 SR **101**

Nach *Absatz 4* können die Daten, die bei Überwachungen des Fernmeldeverkehrs gesammelt wurden, in zwei Fällen wie bisher – wenn möglich verschlüsselt – auf mobilen Datenträgern übermittelt werden. Dies ist zum einen der Fall, wenn die schweizerische Behörde, die mit dem Verfahren befasst ist, diese Daten an eine ausländische Behörde übermitteln muss (*Bst. a*). Es ist nicht wünschenswert, dass ausländische Behörden diese Daten durch einen Online-Zugriff auf das vom Dienst betriebene Verarbeitungssystem abrufen können. Eine Übermittlung auf mobilen Datenträgern kann zum andern auch erfolgen, wenn der Online-Zugriff auf die Daten aufgrund von technischen Problemen nicht möglich ist (*Bst. b*). Zur Verschlüsselung siehe die Erläuterungen zu Artikel 12 Absatz 2.

Art. 10 Akteneinsichtsrecht und Recht auf Auskunft über die Daten

Auch Artikel 10 VE-BÜPF wurde im Vernehmlassungsverfahren von zahlreichen Teilnehmern in Frage gestellt. Vor allem wurde vorgebracht, dieser Artikel sei teilweise unnötig, da die StPO ausreichende Bestimmungen für den Schutz der Personendaten enthalte, und die vorgenommenen Verweise seien überflüssig oder ergäben keinen Sinn. Aus Sicht des Bundesrates ist diese Kritik teilweise berechtigt. Im vorliegenden Entwurf wird deshalb eine überarbeitete Regelung vorgeschlagen, die den obigen Ausführungen Rechnung trägt.

Absatz 1 betrifft die Rechte bezüglich des Zugriffs auf und des Zugangs zu Daten, die im Rahmen eines Strafverfahrens (Art. 1 Abs. 1 Bst. a) oder eines Rechtshilfeersuchens (Art. 1 Abs. 1 Bst. b) gesammelt wurden; bei Letzterem ist es unerheblich, ob es um ein Auslieferungsersuchen oder einen anderen Fall von Rechtshilfe geht. *Absatz 1* unterscheidet zwischen hängigen (*Bst. a*) und abgeschlossenen (*Bst. b*) Verfahren. *Absatz 1 Buchstabe a* verweist für das Akteneinsichts- und Auskunftsrecht im Rahmen eines hängigen Verfahrens auf die anwendbaren Verfahrensbestimmungen. Diese Rechte richten sich demnach nach der Strafprozessordnung oder anderem anwendbaren Verfahrensrecht wie dem MStP. De facto verweist *Absatz 1* auf die Artikel 97, 101 und 279 StPO. *Absatz 1 Buchstabe b* betrifft das Recht auf Auskunft über die Daten nach Abschluss eines Verfahrens. Ist eine Bundesbehörde mit dem Rechtshilfeersuchen befasst, sind in diesen Fällen insbesondere Artikel 8 und 9 des Bundesgesetzes vom 19. Juni 1992[28] über den Datenschutz (DSG) anwendbar. Falls eine kantonale Behörde mit dem Rechtshilfeersuchen befasst ist und das kantonale Recht bezüglich des Auskunftsrechts keinen angemessenen Schutz gewährleistet, findet Artikel 37 Absatz 1 DSG subsidiär Anwendung.

Es gilt auf einige Besonderheiten im Rechtshilfeverfahren hinzuweisen. Sofern die Daten im Rahmen des Vollzugs eines Auslieferungsersuchens gesammelt wurden, richten sich die Rechte der betroffenen Person nach Artikel 18*a* Absatz 4 des Bundesgesetzes vom 20. März 1981[29] über internationale Rechtshilfe in Strafsachen (IRSG), nach den Artikeln 26 und 27 des Bundesgesetzes vom 20. Dezember 1968[30] über das Verwaltungsverfahren (VwVG) – anwendbar gemäss Artikel 12 Absatz 1 erster Satz IRSG – und nach den Artikeln 8 und 9 DSG. In den anderen Fällen von Rechtshilfe richten sich die Rechte der betroffenen Person nach den Artikeln 18*a* Absatz 4 und 80*b* IRSG, nach Artikel 9 des Bundesgesetzes vom 3. Oktober 1975[31]

28 SR **235.1**
29 SR **351.1**
30 SR **172.021**
31 SR **351.93**

zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen und nach Artikel 46 des Bundesgesetzes vom 22. Juni 2001[32] über die Zusammenarbeit mit dem Internationalen Strafgerichtshof (ZISG) sowie entweder nach den Artikeln 8 und 9 DSG (wenn eine Bundesbehörde für das Rechtshilfeersuchen zuständig ist) oder nach dem kantonalen Recht (wenn eine kantonale Behörde dafür zuständig ist). Zu beachten ist, dass das Bundesgesetz vom 21. Dezember 1995[33] über die Zusammenarbeit mit den internationalen Gerichten zur Verfolgung schwerwiegender Verletzungen des humanitären Völkerrechts (Art. 2) und die internationalen Rechtshilfeabkommen, welche die Schweiz mit ausländischen Staaten geschlossen hat (zum Beispiel mit Kanada und Brasilien), die Anwendung des IRSG vorsehen, unter anderem von dessen Artikeln 18*a* Absatz 4 und 80*b*. Ist die für das Rechtshilfeersuchen zuständige Behörde eine kantonale Staatsanwaltschaft, ist möglicherweise Artikel 37 Absatz 1 DSG anwendbar (siehe oben). Sind die Rechte der betroffenen Person eingeschränkt, muss die im Rahmen der Ausübung dieser Rechte zuständige Behörde in der Lage sein, das entsprechende Ersuchen so zu beantworten, dass keine Informationen offenbart werden, die unter das Amtsgeheimnis fallen.

Absatz 2 gilt für das Recht auf Auskunft über die Daten, die bei der Suche nach vermissten (Art. 1 Abs. 1 Bst. c) oder verurteilten (Art. 1 Abs. 1 Bst. d) Personen gesammelt worden sind. Ist die mit dem Verfahren befasste Behörde eine Bundesbehörde, gelten die Artikel 8 und 9 DSG. Wenn eine kantonale Behörde mit dem Verfahren befasst ist und das kantonale Recht keinen angemessenen Schutz gewährleistet, ist Artikel 37 Absatz 1 DSG subsidiär auf das Recht auf Auskunft über die Daten anwendbar, die durch eine Überwachung gesammelt worden sind. Artikel 279 StPO gilt zudem sinngemäss; entsprechend muss die von einer Überwachung betroffene Person informiert werden (durch die Behörde, welche die Überwachung angeordnet hat; siehe die Erläuterungen zu Art. 37 Abs. 2).

Die in *Absatz 3* vorgesehene Regelung bringt klar zum Ausdruck – auch wenn dies selbstverständlich erscheinen mag –, dass der Dienst nur Besitzer der Daten ist. Inhaber der Datensammlung sind nach Artikel 13 die Behörden, die gemäss Artikel 9 Zugriff auf das Verarbeitungssystem haben. Falls die letzte mit dem Verfahren befasste Behörde formell nicht mehr besteht (zum Beispiel im Fall einer Fusion mit einer anderen Behörde oder einer Integration in eine andere Behörde), ist selbstverständlich die ihr nachfolgende Behörde im Sinne von *Absatz 3* zuständig. Falls ein Gesuch um Auskunft über die Daten beim Dienst eingereicht wird, muss dieser das Gesuch unverzüglich an die zuständige Behörde weiterleiten.

Absatz 4 gibt dem Bundesrat den Auftrag, die Einzelheiten der Ausübung der erwähnten Rechte zu regeln und dabei die technischen Besonderheiten des Systems zu berücksichtigen. Es ist insbesondere der Fall zu regeln, in dem die Anfertigung von Kopien der Überwachungsdaten – wie es das anwendbare Verfahrensrecht (hauptsächlich Art. 102 Abs. 3 StPO) vorsieht – technisch problematisch ist, zum Beispiel weil eine besonders grosse Datenmenge kopiert werden soll (siehe auch die einleitenden Erläuterungen zu Ziff. 2.2). Die entsprechenden Bestimmungen werden den betroffenen Kreisen in einer Vernehmlassung bzw. Anhörung unterbreitet.

32 SR **351.6**
33 SR **351.20**

Art. 11 Aufbewahrungsfrist für die Daten

Auch Artikel 11 VE-BÜPF stiess in der Vernehmlassung bei etlichen Teilnehmern auf Kritik. Diese vertraten insbesondere die Auffassung, die vorgeschlagene Regelung, vor allem das geplante Mitteilungssystem, sei zu komplex und kostspielig und verursache unnötigen administrativen Aufwand. Zudem wurde verlangt, die Aufbewahrungsfrist anhand der bestehenden Regeln in der StPO festzulegen, um zu verhindern, dass auf unterschiedliche Regelungen abgestellt werden muss. Der Bundesrat erachtet die geäusserte Kritik teilweise als berechtigt. Im vorliegenden Entwurf wird deshalb eine einfachere Lösung vorgeschlagen. Gegenüber der Regelung, die in Artikel 11 VE-BÜPF vorgesehen war, entsteht für die Behörden, vor allem für die Strafverfolgungsbehörden, ein geringerer administrativer Aufwand.

Absatz 1 betrifft die Daten, die im Rahmen eines Strafverfahrens gesammelt worden sind (Art. 1 Abs. 1 Bst. a): Sein Inhalt ist naheliegend, denn die StPO und das übrige anwendbare Strafverfahrensrecht wie der MStP enthalten angemessene Bestimmungen zur Aufbewahrung von Verfahrensakten. Zudem wäre es widersprüchlich, unterschiedliche anwendbare Regelungen vorzusehen: Eine, die sich aus dem einschlägigen Strafprozessrecht ableitet und eine spezifische, die im BÜPF festgelegt ist. *De facto* verweist *Absatz 1* insbesondere auf das System, das sich aus den Artikeln 99 Absatz 2, 100 und 103 Absatz 1 StPO ableitet. Die Daten sind entweder mittels Aktenverweises oder durch direktes Einfügen im Aktendossier enthalten (Art. 100 StPO). Die Akten sind mindestens bis zum Ablauf der Verfolgungs- und Vollstreckungsverjährung aufzubewahren (Art. 103 Abs. 1 StPO). Demnach müssen die Personendaten in den Akten mindestens solange aufbewahrt werden, bis die Verjährung eintritt (Art. 99 Abs. 2 StPO).

Die in *Absatz 2* vorgesehene Höchstdauer für die Aufbewahrung der Daten nach Artikel 1 Absatz 1 Buchstabe b ist vor allem deshalb gerechtfertigt, weil Rechtshilfeverfahren oft lange dauern. Diese Dauer entspricht den längsten Fristen, die im schweizerischen Recht für die Verfolgungs- und für die Vollstreckungsverjährung vorgesehen sind (abgesehen von den Fällen der Unverjährbarkeit und der Verlängerung der Strafe). Dabei ist überdies zu beachten, dass diese Fristen in einem konkreten Fall kürzer sein können als jene, die im Recht des ersuchenden Staates vorgesehen sind.

In *Absatz 3* ist die Höchstdauer für die Aufbewahrung der Daten nach Artikel 1 Absatz 1 Buchstabe c verankert. Diese Maximalfrist ist namentlich deshalb gerechtfertigt, weil das wertvollste Rechtsgut, d.h. das Leben von Menschen, auf dem Spiel steht und zudem Personen unter Umständen während sehr langer Zeit vermisst bleiben.

Aus den Gründen, die in den Erläuterungen zu Absatz 1 aufgeführt sind, versteht sich der Inhalt von *Absatz 4 erster Satz* (Art. 1 Abs. 1 Bst. d) grundsätzlich von selbst. Auch diese Bestimmung verweist insbesondere auf das System, das sich aus den Artikeln 99 Absatz 2, 100 und 103 Absatz 1 StPO ableitet (siehe im Übrigen die Erläuterungen zu Abs. 1). In *Absatz 4 zweiter Satz* ist die Höchstdauer für die Aufbewahrung der Daten nach Artikel 1 Absatz 1 Buchstabe d verankert. Diese Maximalfrist ist vor allem deshalb gerechtfertigt, weil das wertvollste Rechtsgut, d.h. das Leben von Menschen, auf dem Spiel stehen kann und zudem Personen unter Umständen während sehr langer Zeit nicht aufgefunden werden. In diesem Zusammenhang ist darauf hinzuweisen, dass eine Sanktion in Form einer freiheitsentziehenden Massnahme nicht verjährt. Im Gegensatz dazu ist bei einer Freiheitsstrafe

grundsätzlich eine Verjährung vorgesehen. Wurden die Daten im Rahmen einer Fahndung nach einer Person gesammelt, die sowohl zu einer Freiheitsstrafe verurteilt als auch mit einer freiheitsentziehenden Massnahme sanktioniert wurde, so entspricht die maximale Aufbewahrungsfrist der längeren der beiden anwendbaren Fristen.

Nach *Absatz 5* ist es Sache der mit dem Verfahren befassten Behörde oder, falls keine Behörde mehr mit dem Verfahren befasst ist, der letzten damit befassten Behörde, die notwendigen Schritte zu unternehmen, damit der Dienst die im Verarbeitungssystem aufbewahrten Daten bei Ablauf der Fristen löscht, die in den Absätzen 1–4 festgelegt sind. Im Hinblick darauf muss die zuständige Behörde die Kontrolle dieser Fristen über einen längeren Zeitraum sicherstellen. Für diese Behörden kann dies selbstverständlich mit zusätzlichen administrativen Aufgaben verbunden sein. Der Aufwand ist jedoch vertretbar, da er sich mit einer angemessenen Organisation der Fristenkontrolle in Grenzen halten lässt. Die vorliegende Lösung ist der Regelung vorzuziehen, die in Artikel 11 Absatz 5 VE-BÜPF vorgeschlagen wurde. Bei dieser wäre grundsätzlich der Dienst dafür zuständig, die Einhaltung der in den Absätzen 1–4 festgelegten Fristen zu kontrollieren und die mit dem Verfahren befasste Behörde (oder die letzte damit befasste Behörde) über eine zentrale Behörde vom bevorstehenden Ablauf der Frist in Kenntnis zu setzen. Diese Regelung hätte deshalb sowohl für den Dienst als auch für die oben erwähnten Behörden einen unverhältnismässigen administrativen Aufwand zur Folge. Die verschiedenen Behörden müssten zunächst dem Dienst für jede Überwachung die anwendbaren Fristen nach den Absätzen 1–4 mitteilen. Diese Mitteilung wäre unerlässlich, denn je nach Inhalt des Verfahrens ist diese Frist unterschiedlich lang (zum Beispiel hängt die Frist der Verfolgungsverjährung von der Strafe ab, die für die strafbare Handlung vorgesehen ist, und die verhängte Strafe wirkt sich auf die Frist der Vollstreckungsverjährung aus); ausserdem hat der Dienst keinen Zugang zu den Akten. Es ist auch zu berücksichtigen, dass sich die jeweilige strafbare Handlung sowie die verhängte Strafe und folglich auch die Aufbewahrungsfrist auf dem Weg durch die verschiedenen Instanzen ändern können. Dies würde dem Dienst die Fristenkontrolle weiter erschweren. Zudem liegt es auf der Hand, dass die erwähnten Schritte nicht vom Dienst, sondern von der mit dem Verfahren befassten Behörde (oder der letzten damit befassten Behörde) unternommen werden müssen, da diese als Inhaber der Datensammlung gilt (siehe Art. 13). Die mit dem Verfahren befasste Behörde oder die letzte damit befasste Behörde informiert den Dienst auch, falls nach geltendem Recht eine Übertragung der Daten erfolgen muss, bevor der Dienst diese aus dem Verarbeitungssystem löscht. Dabei geht es insbesondere um die Einhaltung allfälliger Archivierungsvorschriften von Bund oder Kantonen. Im Bereich der Archivierung gelangen die Bestimmungen derjenigen Gebietskörperschaft (Bund oder Kanton) zur Anwendung, der die mit dem Verfahren befasste Behörde (oder die letzte damit befasste Behörde) angehört, da diese Inhaber der Datensammlung ist (siehe Art. 13). Für die Bedeutung des Ausdrucks «mit dem Verfahren befasste Behörde», siehe die Erläuterungen zu Artikel 10 Absatz 3.

Die Pflicht des Dienstes, die zuständige Behörde 30 Jahre nach Abschluss der Überwachung zu kontaktieren, um abzuklären, wie mit den noch vorhandenen Daten verfahren werden soll, ist eine reine Vorsichtsmassnahme. Sie soll sicherstellen, dass die Daten in Übereinstimmung mit Absatz 1–4 gelöscht werden, selbst wenn die zuständige Behörde es versäumt haben sollte, den Dienst über den Umgang mit den Daten zu informieren.

In Ausübung seiner Kompetenz nach *Absatz 6* wird der Bundesrat namentlich auf die technischen Besonderheiten des Verarbeitungssystems Rücksicht nehmen. Er kann beispielsweise vorsehen, dass die betroffene Strafverfolgungsbehörde die Aufbewahrungsfrist für alle oder einen Teil ihrer Daten selber im Verarbeitungssystem erfasst und dass diese Behörde den Dienst eine bestimmte Anzahl Tage vor Ablauf der Aufbewahrungsfrist kontaktiert und instruiert, damit dem Dienst genügend Zeit für die Ausführung der Instruktionen bleibt. Der Bundesrat kann beispielsweise auch vorsehen, dass alle oder ein Teil der Daten automatisch gelöscht werden, falls die betroffene Behörde den Dienst nicht innert nützlicher Frist kontaktiert.

Art. 12 Sicherheit

Die in *Absatz 1* vorgesehene Regelung ist sachgerecht, weil der Dienst – selbst wenn er nicht Inhaber der Datensammlung ist (siehe auch die Erläuterungen zu Art. 13) – das Verarbeitungssystem betreibt, in dem die Daten gespeichert sind; er gilt somit als Besitzer der Daten.

Gestützt auf *Absatz 2* kann der Bundesrat namentlich Vorschriften zur Kontrolle des Zugriffs auf die Daten erlassen sowie zur Frage, wann diese verschlüsselt werden müssen (siehe ebenfalls Art. 9 und die entsprechenden Erläuterungen). Die vom Bundesrat gestützt auf *Absatz 2* vorgeschlagenen Vorschriften werden den betroffenen Kreisen in einer Vernehmlassung bzw. Anhörung unterbreitet.

Absatz 3 lehnt sich an Artikel 9 Absatz 2 der geltenden VÜPF an. Unter Datensicherheit nach dieser Bestimmung ist insbesondere die Vertraulichkeit und Vollständigkeit der Daten zu verstehen.

Art. 13 Verantwortung

Artikel 13 legt fest, dass die Behörden, die Zugriff zum Verarbeitungssystem haben, als Inhaber der Datensammlung gelten, nicht der Dienst, der nur als Besitzer der im Verarbeitungssystem gespeicherten Daten gilt und nur für die Gewährung der entsprechenden Zugriffsrechte zuständig ist (siehe auch die Erläuterungen zu Art. 9 und 12).

Art. 14 Schnittstelle zum polizeilichen Informationssystem-Verbund des Bundesamtes für Polizei

Absatz 1 bildet eine ausdrückliche Rechtsgrundlage für das elektronische Kopieren und Übermitteln der Daten aus dem Informatiksystem, das der Dienst zur Verarbeitung der im Rahmen einer Fernmeldeüberwachung gesammelten Daten betreibt, in den polizeilichen Informationssystem-Verbund gemäss Artikel 10, 12 und 13 BPI. Damit wird die Bearbeitung dieser Daten in diesem Informationssystem-Verbund ermöglicht. Damit der Datentransfer durchgeführt werden darf, ist es erforderlich, dass das anwendbare Recht die entsprechende Datenbearbeitung in den jeweiligen Systemen erlaubt (*Bst. a*).

Einzig den mit einem konkreten Verfahren befassten Personen wird die Bearbeitung der entsprechenden Daten im jeweiligen Informationssystem gemäss BPI gestattet (*Bst. b*). Dieser Punkt müsste an sich im BPI geregelt werden, was sich aber aus Gründen der gesetzgeberischen Systematik nur unbefriedigend umsetzen lässt. Eine Revision des BPI ist angestrebt, bei der die Frage des Zugangs zu den Daten im

Informationssystem-Verbund im BPI am systematisch richtigen Ort im Sinne der hier vorgeschlagenen Lösung geregelt werden kann.

Der polizeiliche Informationssystem-Verbund wird von fedpol betrieben. Er dient diesem und den kantonalen Polizeibehörden vor allem zur Auswertung der Informationen, die im Rahmen von Strafuntersuchungen beschafft wurden. Dazu gehören auch die Daten, die durch Überwachungen des Fernmeldeverkehrs gesammelt werden. Gegenüber dem Kopieren und der Übermittlung «von Hand» bieten das Kopieren und die Übermittlung auf elektronischem Weg mehrere Vorteile; unter anderem kann so Zeit und Geld gespart und eine höhere Datensicherheit erreicht werden (verringertes Risiko von Datenverlusten und verringertes Risiko von Fehlern, die sich negativ auf die Datenqualität auswirken können). Die Daten aus dem vom Dienst betriebenen System bleiben nach der Übermittlung in den Informationssystem-Verbund gemäss BPI in beiden Systemen, weshalb von «kopieren» gesprochen wird.

Nach *Absatz 2* wird das Kopieren und Übermitteln der Daten nach Absatz 1 durch einen Befehl von einer Person ausgelöst, die über die Zugriffsrechte auf das vom Dienst betriebene Verarbeitungssystem (Art. 9) und auch auf das entsprechende Informationssystem gemäss BPI verfügt. Diese Übertragungsart darf keinesfalls dazu führen, dass die Zugriffsregeln auf das Informatiksystem des Dienstes und diejenigen auf das Informationssystem gemäss BPI unterwandert werden. Für die Rechtmässigkeit des Kopierens und Übermittelns der Daten aus dem Verarbeitungssystem des Dienstes in den polizeilichen Informationssystem-Verbund gemäss BPI ist nicht der Dienst zuständig, sondern die Strafverfolgungsbehörde.

2.3 3. Abschnitt: Aufgaben des Dienstes

Die Aufgaben des Dienstes stehen in Verbindung mit der Durchführung der Anordnungen zur Überwachung des Post- und Fernmeldeverkehrs. Mit dem Entwurf werden dem Dienst hingegen keine normsetzenden und regulativen Befugnisse in Bezug auf die Durchführung der Überwachungen übertragen; diese Zuständigkeiten kommen dem EJPD zu (Art. 31 Abs. 3). Damit wird der Forderung in Ziffer 1 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision) entsprochen. In diesen Vorstössen wird verlangt, dass die normsetzenden und regulativen Aufgaben des Dienstes grundsätzlich von seinen Aufgaben im Zusammenhang mit der Durchführung der Überwachungen zu trennen sind.

Art. 15 Auskünfte über Fernmeldedienste

Artikel 15 entspricht im Wesentlichen Artikel 14 Absatz 2 und 2bis des geltenden BÜPF, mit Ausnahme des dort enthaltenen Verweises (siehe die Erläuterungen zu Art. 21). Der Begriff der «(Fernmelde-)Anschlüsse» wurde allerdings bisher in einem weiteren Sinn verstanden. Es erschien nun aber angezeigt, ihn im vorliegenden Entwurf durch «(Fernmelde-)Dienste» zu ersetzen. Dies deshalb, weil sich der Begriff «(Fernmelde-)Anschlüsse» mit der technischen Entwicklung als zu eng erwiesen hat. Eine Person erhält von einer Anbieterin lediglich einen Dienst oder eine Anwendung geboten, kann von ihr aber keinen bestimmten Anschluss verlan-

gen. Die erfassten Fernmeldedienste umfassen auch die Internetdienste (siehe auch die Erläuterungen zu Art. 1 Abs. 1).

Absatz 1 Buchstabe a wurde gegenüber Artikel 14 Absatz 2 Buchstabe a des geltenden BÜPF ergänzt. Entgegen dem Wortlaut der letzteren Bestimmung, die wahrscheinlich auf ein Versehen des Gesetzgebers zurückzuführen ist, müssen die Auskünfte selbstverständlich nicht nur zur Bestimmung der zu überwachenden Dienste und Personen angefordert werden können, um diese unter Überwachung zu stellen. Es muss vielmehr auch möglich sein, Auskünfte zu verlangen, um zu bestimmen, wer mit dem überwachten Dienst in Verbindung steht. Dies gilt auch für den Fall, dass keine Überwachung der Dienste aller dieser Gesprächspartner gewünscht wird[34]. Um den Anforderungen des Legalitätsprinzips besser gerecht zu werden, wird präzisiert, dass die Daten nicht mehr ausschliesslich den Behörden geliefert werden können, welche eine Überwachung anordnen oder genehmigen dürfen, sondern auch den von diesen bezeichneten (Strafverfolgungs-) Behörden. Damit kann insbesondere auch die Polizei, die in der Praxis grundsätzlich mit der Auswertung der Daten beauftragt wird, diese Daten erhalten.

Absatz 1 Buchstabe b wird aus Artikel 14 Absatz 2 Buchstabe b des geltenden BÜPF übernommen. Diese Bestimmung betrifft nicht nur die polizeilichen Aufgaben im Zusammenhang mit Strafverfahren, sondern auch die Aufgaben, welche die Polizei ausserhalb solcher Verfahren erfüllt[35]. Die Bestimmung bedeutet auch, dass es keine Anordnung der Staatsanwaltschaft braucht, damit die in der Bestimmung erwähnten Polizeidienste die betreffenden Daten erhalten, welche nicht dem Fernmeldegeheimnis unterstehen und deren Beschaffung keine Zwangsmassnahme darstellt (siehe die Erläuterungen zu Art. 21). Die Polizeidienste können insbesondere im Rahmen von Artikel 306 f. StPO von sich aus beim Dienst die betreffenden Auskünfte verlangen und bei diesem beschaffen.

Absatz 1 Buchstabe c entspricht Artikel 14 Absatz 2 Buchstabe c des geltenden BÜPF.

Absatz *2 Buchstabe a* übernimmt sinngemäss Artikel 14 Absatz 2bis des geltenden BÜPF; der dort enthaltene Verweis wird an die geänderte Struktur des Entwurfs angepasst.

Artikel 23 des Bundesgesetzes vom 19. Dezember 1986[36] gegen den unlauteren Wettbewerb (UWG) in Verbindung mit Artikel 10 Absatz 3 UWG überträgt dem Bund das Strafantragsrecht betreffend unlauterer Verhaltensweisen, falls Gemeininteressen betroffen sind. Nach geltendem Recht ist die Ausübung dieses Strafantragsrechts in Fällen von unerwünschten Werbeanrufen gemäss Artikel 3 Absatz 1 Buchstabe u UWG ausserordentlich schwierig. Weil die anrufenden Werbeunternehmen (bzw. deren Call-Center) ihren Telefonanschluss offenbar regelmässig wechseln oder über mehrere verschiedene Rufnummern verfügen, liegt bei der zuständigen Bundesbehörde oft nur eine einzige Beschwerde gegen eine einzige Rufnummer vor. Dies hat zur Folge, dass der Bund mangels Gemeininteresse nicht strafantragsberechtigt ist. Es ist aber davon auszugehen, dass hinter verschiedenen Rufnummern oft dasselbe Unternehmen steckt. Damit die Bundesbehörde ihr Strafantragsrecht wahrnehmen und unerwünschte Werbeanrufe effektiv bekämpfen kann, ist es not-

34 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 14 BÜPF N 16.
35 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 14 BÜPF N 18; siehe Botschaft vom 1. Juli 1998 betreffend das geltende BÜPF, BBl **1998** 4279.
36 SR **241**

wendig, dass sie inskünftig die Daten gemäss Absatz 2 Buchstabe b erhält. Das Strafantragsrecht des Bundes im oben ausgeführten Sinn wird durch das Staatssekretariat für Wirtschaft ausgeübt[37].

Art. 16 Allgemeine Aufgaben bei der Überwachung

In *Artikel 16* sind die Aufgaben aufgeführt, die dem Dienst im Bereich der Überwachung des Post- und Fernmeldeverkehrs zukommen. Diese Aufgaben werden aus den Artikeln 11 und 13 des geltenden BÜPF übernommen. Im Gegensatz zur Regelung im geltenden BÜPF ist künftig kein Artikel zu den spezifischen Aufgaben des Dienstes im Bereich der Überwachung des Postverkehrs mehr vorgesehen. Für die Überwachung des Fernmeldeverkehrs bestehen hingegen weiterhin spezifische Bestimmungen (siehe die Erläuterungen zu Art. 17).

Buchstabe a orientiert sich an den Artikeln 11 Absatz 1 Buchstabe a und 13 Absatz 1 Buchstabe a des geltenden BÜPF. Er betrifft die formelle Prüfung, der die Überwachungsanordnung vom Dienst unterzogen wird. Diese Bestimmung begründet im Grunde genommen eine Koordinationsaufgabe des Dienstes. Die Überprüfung bezieht sich auch auf die Vollständigkeit und Klarheit der Überwachungsanordnung[38]. Wie dies schon heute der Fall ist, muss der Dienst insbesondere prüfen, ob die jeweilige Straftat im Katalog der überwachungsfähigen Delikte enthalten ist. Damit die Überwachungsanordnung gegebenenfalls so rasch als möglich berichtigt werden kann, muss sich der Dienst direkt an die anordnende Behörde wenden können (zusätzlich muss die Genehmigungsbehörde im Hinblick auf ihren Entscheid über die erlassene Anordnung über diese Kontaktnahme informiert werden); dies ist vor allem dann angezeigt, wenn der Dienst zum Schluss gelangt, dass nicht klar ist, was in der Überwachungsanordnung verlangt wird. Bei Bedarf kann der Bundesrat die Frist, innerhalb der sich der Dienst mit der oben erwähnten Behörde in Verbindung setzen muss, auf Verordnungsstufe regeln. Trotz dieser Aufgabe des Dienstes (Anzeigepflicht) ist die anordnende Behörde dafür zuständig, dass die Überwachungsanordnung keinen Mangel aufweist; dies ist umso mehr gerechtfertigt, als die Behörde nicht verpflichtet ist, die Meinung des Dienstes zu beachten. Siehe dazu sinngemäss die Erläuterungen zu Buchstabe b.

Buchstabe b sieht vor, dass der Dienst die Überwachungsanordnung einer materiellen Prüfung unter dem Gesichtspunkt des Verwaltungsrechts unterzieht. Auch diese Bestimmung begründet im Grunde genommen eine Koordinationsaufgabe des Dienstes. Im Vergleich zur Regelung, die im VE-BÜPF für die Überwachung des Fernmeldeverkehrs vorgesehen war, wird mit dem vorliegenden Entwurf die Prüfungsbefugnis des Dienstes erweitert. Damit wird einer Forderung entsprochen, die zahlreiche Vernehmlassungsteilnehmer geäussert hatten. Diese Bestimmung ist nicht darauf ausgerichtet, die Überwachungsanordnung einer materiellen Prüfung hinsichtlich der anwendbaren Strafprozessbestimmungen zu unterziehen, die in den Artikeln 269 ff. StPO oder 70 ff. MStP festgelegt sind, d.h. rein strafprozessuale Fragen zu prüfen. Somit ist es beispielsweise nicht Sache des Dienstes, zu bestimmen, ob von der angeordneten Überwachung verwertbare Resultate zu erwarten sind, die für eine bestimmte Strafuntersuchung von Belang sind. Denn diese Prüfung

37 Siehe Artikel 1 Absatz 1 der Verordnung vom 12. Oktober 2011 über das Klagerecht des Bundes im Rahmen des Bundesgesetzes gegen den unlauteren Wettbewerb (SR **241.3**).
38 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 11 BÜPF N 2–10.

ist ausschliesslich Sache der Genehmigungsbehörde (siehe auch die Erläuterungen zu Art. 42 Abs. 2).

Mit der Aufgabe des Dienstes, die in *Buchstabe b* erwähnt ist, soll verhindert werden, dass der Dienst einer Person, die in den persönlichen Geltungsbereich des Gesetzes fällt, eine Überwachungsanordnung übermitteln muss, die seiner Meinung nach eine in dieser Bestimmung erwähnte Eigenschaft aufweist, ohne dass er zuvor die anordnende Behörde und die Genehmigungsbehörde darauf aufmerksam gemacht hat. Dieser Mechanismus soll der anordnenden Behörde und der Genehmigungsbehörde insbesondere ermöglichen, einfacher von den Problemen Kenntnis zu erhalten, die mit einer solchen Überwachungsanordnung verbunden sind. Die anordnende Behörde und die Genehmigungsbehörde können die Meinung des Dienstes beachten und die Anordnung im konkreten Fall widerrufen beziehungsweise sie nicht genehmigen; sie sind aber nicht dazu verpflichtet. Die Verfechter eines Rechtsmittels (Einsprache- oder Beschwerdeverfahren) zur Klärung von Meinungsverschiedenheiten zwischen dem Dienst und der anordnenden Behörde sind der Ansicht, dass dieser Kontrollmechanismus (Anzeigepflicht des Dienstes) nicht ausreicht. Sie führen insbesondere an, dass erfahrungsgemäss nicht alle Divergenzen im Dialog behoben werden können. Ihrer Meinung nach wäre es auch nicht logisch, dass der Dienst in Bezug auf die Überwachungsverfügung eine eingeschränkte Kognition haben soll, während die Beschwerdeinstanz, die allenfalls von einer mit der Verfügung nicht einverstandenen Fernmeldedienstanbieterin angerufen wird, mit voller Kognition entscheiden könnte. Der vorgeschlagene neue Kontrollmechanismus (Anzeigepflicht des Dienstes) erscheint jedoch als notwendig und hinreichend, um insbesondere die unnötigen Komplikationen zu verhindern, die sich daraus ergeben können, dass z.B. eine Anbieterin von Fernmeldediensten Beschwerde gegen die Verfügung des Dienstes einlegt, mit der die Durchführung einer Überwachung mit den Merkmalen nach *Buchstabe b* verlangt wird. Hingegen ist es nicht notwendig, ein Rechtsmittel, selbst ohne aufschiebende Wirkung, zur Klärung eventueller Meinungsverschiedenheiten zwischen dem Dienst und der anordnenden Behörde einzuführen. Denn es darf nicht vergessen werden, dass der Dienst eigentlich eine Vollzugsbehörde ist, eine Schnittstelle zwischen den Strafverfolgungsbehörden und den Fernmeldedienstanbieterinnen. Ein solches Rechtsmittel wäre demnach systemwidrig. Es ist darauf hinzuweisen, dass der Dienst die volle Kompetenz hat, die Überwachungsanordnung – welche die Grundlage für die Überwachungsverfügung an eine Fernmeldedienstanbieterin bildet – in verwaltungsrechtlicher Hinsicht zu prüfen und gegebenenfalls zu ergänzen. Der Dienst verfügt daher nicht über eine «eingeschränkte Kognition» im Vergleich zum Bundesverwaltungsgericht. Ausserdem führt der Dialog zwischen dem Dienst und den Strafverfolgungsbehörden, der sich aus *Buchstabe b* unweigerlich ergibt, zu einer Art Wiedererwägung der Überwachungsanordnungen von Gesetzes wegen. Dabei dürfen auch die zu erwartenden Fortschritte dank des neuen Instruments des beratenden Organs nach Artikel 5 nicht aus den Augen verloren werden. Die Strafverfolgungsbehörden werden im Rahmen dieses Organs insbesondere über die technischen Möglichkeiten informiert werden können, und der Dienst wird den Nutzen der angeordneten Überwachungen besser erkennen können. Die an den Dienst übermittelte Überwachungsanordnung ist im Übrigen Gegenstand einer Überprüfung durch eine gerichtliche Behörde, nämlich durch das Zwangsmassnahmengericht (Art. 274 StPO), dem der Dienst nach *Buchstabe b* auch seine Stellungnahme übermitteln muss. Diese unabhängige Behörde kann durchaus entscheiden, die angeordnete Überwachung aus strafprozessualen Gründen nicht zu genehmigen. Die gesammelten Daten sind

diesfalls grundsätzlich zu vernichten und sind nicht verwertbar (Art. 277 StPO). Die Einführung eines Rechtsmittels zur Klärung von Meinungsverschiedenheiten zwischen dem Dienst und der anordnenden Behörde ist umso weniger gerechtfertigt, als die Anbieterinnen von Fernmeldediensten die Möglichkeit haben, sich im Rahmen von Artikel 42 Absatz 2 gegen die vom Dienst weitergeleiteten Überwachungsanordnungen vor dem Bundesverwaltungsgericht zur Wehr zu setzen. Nebst dem Dienst kann auch die Behörde, welche die Überwachung angeordnet hat, vom Bundesverwaltungsgericht aufgefordert werden, sich zur Überwachungsanordnung zu äussern. Eine solche Beschwerde kann dazu führen, dass die von der Strafverfolgungsbehörde angeordnete Überwachung von der betreffenden Fernmeldedienstanbieterin nicht selber durchgeführt werden muss (für Einzelheiten siehe die Erläuterungen zu Art. 42). Schliesslich ist zu erwähnen, dass trotz dieser Aufgabe des Dienstes (Anzeigepflicht) die anordnende Behörde dafür zuständig ist, dass die Überwachungsanordnung keinen Mangel aufweist; dies ist umso mehr gerechtfertigt, als die Behörde nicht verpflichtet ist, die Meinung des Dienstes zu beachten.

Als ungeeignet im Sinne von *Buchstabe b* gelten jene Überwachungsanordnungen, die angesichts der technischen Merkmale des Einzelfalls nicht zu verwertbaren Ergebnissen führen können. Für die Klärung der Frage, ob eine Überwachung unter einen im Gesetz vorgesehenen Überwachungstyp fällt, sind insbesondere das BÜPF, die VÜPF und die StPO massgebend. An dieser Stelle ist festzuhalten, dass der Dienst bei der Abklärung der technischen Machbarkeit der Überwachung nicht darauf abstellen muss, ob die Person, welche die Verfügung ausführen muss, über die dazu notwendigen technischen Möglichkeiten verfügt. Das entscheidende Kriterium ist vielmehr der Stand der Technik zum Zeitpunkt, an dem die Überwachung ausgeführt werden soll. Wenn die Person nicht in der Lage ist, die Überwachung auszuführen, kann der Dienst diese selber ausführen oder die Ausführung einem Dritten übertragen (siehe Art. 34 Abs. 1 und die entsprechenden Erläuterungen).

Selbstverständlich muss die in *Buchstabe b* erwähnte Frist, innerhalb welcher der Dienst die anordnende Behörde und die Genehmigungsbehörde informieren muss, sehr kurz bemessen sein, damit insbesondere die anordnende Behörde gegebenenfalls rasch eine andere Überwachung anordnen kann. Bei Bedarf kann der Bundesrat diese Frist regeln.

Die in *Buchstabe c* erwähnte Aufgabe des Dienstes ist in Verbindung mit den Artikeln 20 und 24 zu betrachten. Im Gegensatz zum Fall, der in Artikel 26 Absatz 2 vorliegt, geht es hier darum, Informationen zu erhalten, bevor eine Überwachung angeordnet wird.

Buchstabe d entspricht im Wesentlichen den Artikeln 11 Absatz 1 Buchstabe b und 13 Absatz 1 Buchstabe b des geltenden BÜPF. Diese Bestimmung weist eine gewisse Ähnlichkeit mit Artikel 33 Absatz 5 auf. Dieser Artikel bezieht sich jedoch nicht auf ein Verfahren im Zusammenhang mit der Ausführung einer Überwachung, sondern auf ein Verfahren zum Nachweis der Auskunfts- und Überwachungsbereitschaft. Dieses kann auch im Anschluss an eine Überwachung erfolgen, die nicht optimal verlaufen ist. Dass die Aufgabe, die Ausführung der Überwachung zu kontrollieren, erwähnt wird, unterstreicht die Funktion des Dienstes als Mittler zwischen den Strafverfolgungsbehörden und den Anbieterinnen von Fernmeldediensten.

Buchstabe e entspricht im Wesentlichen Artikel 13 Absatz 1 Buchstabe f des geltenden BÜPF, der auf die Überwachung des Fernmeldeverkehrs anwendbar ist. 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 Berufsgeheimnis geschützt werden muss, von dem die Strafverfolgungsbehörde nicht Kenntnis erhalten darf (siehe die Erläuterungen zu Art. 271 StPO und 70*b* MStP). Der Dienst trifft die notwendigen Vorkehren für die Umsetzung der Massnahmen, die im Rahmen der oben aufgeführten Artikel beschlossen wurden; er nimmt aber zum Beispiel nicht selbst die Aussonderung vor, die in diesen Artikeln erwähnt ist (Art. 271 Abs. 1 StPO und Art. 70*b* Abs. 1 MStP).

Buchstabe f lehnt sich an die Artikel 11 Absatz 1 Buchstabe d und 13 Absatz 1 Buchstabe g des geltenden BÜPF an. Der Dienst muss nun ein Schriftstück erhalten, d.h. eine Kopie des Verlängerungsgesuchs.

Buchstabe g entspricht den Artikeln 11 Absatz 1 Buchstabe c und 13 Absatz 1 Buchstabe h des geltenden BÜPF.

Buchstabe h entspricht den Artikeln 11 Absatz 1 Buchstabe g und 13 Absatz 1 Buchstabe k des geltenden BÜPF.

Buchstabe i entspricht einem Bedürfnis aufgrund der Komplexität des Verarbeitungssystems.

Buchstabe j entspricht im Wesentlichen den Artikeln 11 Absatz 2 Satz 1 und 13 Absatz 2 Buchstabe e des geltenden BÜPF und ergänzt diese mit der Beratung zu operativen Aspekten.

Die Aufgaben nach Artikel 13 Absatz 2 Buchstabe a–d des geltenden BÜPF werden nicht in *Artikel 16* übernommen. Es handelt sich dabei nicht mehr um Aufgaben, die vom Dienst auf Ersuchen wahrgenommen werden müssen oder die von diesem noch erwartet werden dürfen, weil für bestimmte Aufgaben zu wenig Mittel zur Verfügung stehen, während andere nicht mehr notwendig sind.

Art. 17 Aufgaben bei der Überwachung des Fernmeldeverkehrs

In Artikel 17 sind die Aufgaben des Dienstes aufgeführt, die spezifisch mit den angeordneten Überwachungen im Bereich des Fernmeldeverkehrs zusammenhängen, unter Ausschluss des Postverkehrs. Dieser Artikel ist auch auf bestimmte Anbieterinnen abgeleiteter Kommunikationsdienste anwendbar, sofern der Bundesrat von seiner Kompetenz gemäss Artikel 27 Absatz 3 Gebrauch macht (siehe Art. 27 Abs. 3 und die entsprechenden Erläuterungen).

Buchstabe a lehnt sich an Artikel 15 Absatz 2 erster Satz des geltenden BÜPF an. Der dort benutzte Begriff «Nummer» könnte im Prinzip durch den Begriff «Anschluss» ersetzt werden, da er im Zusammenhang mit dem Internetverkehr nicht angemessen ist. Angesichts der technischen Entwicklung der letzten Jahre ist es jedoch angezeigt, diesen Begriff durch «Dienste» zu ersetzen (siehe Erläuterungen zu Art. 15 *in initio*). Weiterhin gilt jedoch das Prinzip, dass mit der Überwachung grundsätzlich jene Anbieterin von Fernmeldediensten beauftragt werden muss, die für die Verwaltung des Dienstes zuständig ist. *Buchstabe a* setzt natürlich voraus, dass der Dienst in der Lage ist einzuschätzen, welcher Fernmeldedienstanbieterin die technische Durchführung der Überwachung den geringsten Aufwand bereitet, was nicht immer möglich ist. Der Dienst orientiert sich bei der Erteilung des Überwachungsauftrags an der Anweisung der anordnenden Behörde. Diese Anweisung ist

jedoch nicht bindend: Die anordnende Behörde soll solche Aspekte grundsätzlich nicht verbindlich festlegen. Der Dienst hat kraft seiner Stellung und seiner Aufgaben die Kompetenz – allenfalls nach Rücksprache mit der anordnenden Behörde, vgl. Artikel 16 Buchstabe b oder Buchstabe a Ziffer 3 –, die geeignete Anbieterin zu bestimmen. Vorgängig muss der Dienst dieser Behörde die Informationen erteilen, die er beschaffen kann, damit diese eine Überwachung anordnen kann (Art. 16 Bst. c).

Buchstabe b geht vom Wortlaut von Artikel 13 Absatz 1 Buchstabe c des geltenden BÜPF aus. Dieser Wortlaut wird an die Betriebsweise des neuen Informatiksystems zur Verarbeitung der Daten, die im Rahmen der Überwachung des Fernmeldeverkehrs gesammelt werden, angepasst. Neu ist grundsätzlich nicht mehr vorgesehen, dass diese Daten den betreffenden Behörden durch den Versand von Datenträgern und Dokumenten auf dem Postweg zur Verfügung gestellt werden. Vielmehr können die Daten nun über einen Online-Zugriff auf das Verarbeitungssystem abgerufen werden (siehe Art. 6 ff.). Um den Anforderungen des Legalitätsprinzips gerecht zu werden, wird zudem in Anlehnung an den Inhalt der Artikel 15 Absatz 1 Buchstabe b und 23 Buchstabe b der geltenden VÜPF in der Bestimmung festgehalten, dass der Dienst nicht mehr nur der anordnenden Behörde, sondern auch der von dieser bezeichneten (Strafverfolgungs-)Behörde Einsicht in den Fernmeldeverkehr gewährt. In diesen Fernmeldeverkehr kann somit insbesondere die Polizei Einsicht nehmen, das sie in der Praxis grundsätzlich sie mit der Auswertung des überwachten Fernmeldeverkehrs beauftragt wird.

Buchstabe c ändert und ergänzt den Wortlaut von Artikel 13 Absatz 1 Buchstabe d des geltenden BÜPF, der den Sonder- und Ausnahmefall regelt, dass eine Überwachung in Form einer Direktschaltung durchgeführt wird. Die Daten, die im Rahmen einer angeordneten Überwachung beschafft werden, laufen grundsätzlich über den Dienst. Dieser bildet die Schnittstelle zwischen den Fernmeldedienstanbieterinnen, die mit der Ausführung der Überwachungen beauftragt sind, und den Behörden, welche die Überwachungen angeordnet haben. Die Daten werden im Verarbeitungssystem aufgezeichnet, das vom Dienst betrieben wird. Dies ist auch dann der Fall, wenn es sich bei der angeordneten Überwachung um eine sogenannte Echtzeit-Überwachung handelt, d.h. wenn es nicht um eine rückwirkende Überwachung geht. Erfolgt die Ausführung der angeordneten Überwachung in Form einer Direktschaltung, übermittelt die Fernmeldedienstanbieterin die beschafften Daten ohne Umweg über den Dienst direkt an die betreffende Behörde, was die Aufzeichnung dieser Daten im vom Dienst betriebenen Verarbeitungssystem ausschliesst. Die betreffende Behörde zeichnet die Daten somit selbst auf. *Buchstabe c* legt fest, unter welchen Bedingungen im Rahmen einer Überwachung eine Direktschaltung verwendet werden kann. Die Fälle, in denen eine Direktschaltung in Anspruch genommen werden kann, entsprechen den Situationen, in denen der Dienst aus technischen Gründen nicht in der Lage ist, die Funktion einer Schnittstelle zwischen den Fernmeldedienstanbieterinnen und den betreffenden Behörden wahrzunehmen, die ihm das Gesetz zuweist. Artikel 271 Absatz 2 StPO und Artikel 70*b* Absatz 2 MStP in der Fassung der StPO bleiben vorbehalten. Dieser restriktive Einsatz der Direktschaltung wird die Wirksamkeit der Arbeit der Strafverfolgungsbehörden nicht beeinträchtigen, da er keine Verzögerungen zur Folge hat: Die Daten, die im Rahmen einer Echtzeit-Überwachung beschafft werden, die nicht über eine Direktschaltung erfolgt, werden den betreffenden Behörden unverzüglich, mit einer Verzögerung von wenigen Sekundenbruchteilen, über das vom Dienst betriebene Verar-

beitungssystem zur Verfügung gestellt. Um den Anforderungen des Legalitätsprinzips besser gerecht zu werden, wird in Anlehnung an den Inhalt der Artikel 15 Absatz 1 Buchstabe b und 23 Buchstabe b der geltenden VÜPF in der Bestimmung festgehalten, dass der Fernmeldeverkehr nicht mehr nur der anordnenden Behörde, sondern auch der von dieser bezeichneten (Strafverfolgungs-)Behörde direkt zugeleitet werden kann. Dieser Fernmeldeverkehr kann somit insbesondere direkt der Polizei zugeleitet werden, die grundsätzlich mit der Auswertung des überwachten Fernmeldeverkehrs beauftragt wird.

Buchstabe d lehnt sich an Artikel 13 Absatz 1 Buchstabe e des geltenden BÜPF an. Der Begriff der Randdaten wird darin gegenüber dem Begriff im geltenden BÜPF angepasst. Die Erläuterungen zu Artikel 26 Absatz 1 Buchstabe b führen Gründe für diese Änderungen und den Umfang der Änderungen auf. In *Buchstabe d* wird der Wortlaut von Artikel 13 Absatz 1 Buchstabe e des geltenden BÜPF an die Betriebsweise des neuen Informatiksystems zur Verarbeitung der Daten angepasst, die im Rahmen der Überwachung des Fernmeldeverkehrs gesammelt werden. Neu ist grundsätzlich nicht mehr vorgesehen, dass diese Daten den betreffenden Behörden durch den Versand von Datenträgern und Dokumenten auf dem Postweg zur Verfügung gestellt werden. Vielmehr können die Daten nun über einen Online-Zugriff auf das Verarbeitungssystem abgerufen werden (siehe Art. 6 ff.). Um den Anforderungen des Legalitätsprinzips gerecht zu werden, wird zudem in Anlehnung an den Inhalt der Artikel 15 Absatz 1 Buchstabe b und 23 Buchstabe b der geltenden VÜPF in der Bestimmung festgehalten, dass der Dienst nicht mehr nur der anordnenden Behörde, sondern auch der von dieser bezeichneten (Strafverfolgungs-)Behörde Einsicht in die betreffenden Daten gewährt. In diese Daten kann somit insbesondere die Polizei Einsicht nehmen, da sie grundsätzlich sie mit der Auswertung des überwachten Fernmeldeverkehrs beauftragt wird.

Die in *Buchstabe e* verankerte Aufgabe ergibt sich aus den vom Dienst zu treffenden Massnahmen nach den Artikeln, die in dieser Bestimmung zitiert sind.

Buchstabe f verweist auf die Artikel 32–34.

Die in *Buchstabe g* vorgesehene Sortierung – die sich von der Aussonderung nach Artikel 271 StPO und 70*b* MStP in Zusammenhang mit dem Schutz des Berufsgeheimnisses unterscheidet – kann nur auf Ersuchen der Behörde erfolgen, welche die Überwachung angeordnet hat. Der Dienst kann nur eine automatische Sortierung vornehmen; jede andere Art der Aussonderung wäre sehr kompliziert oder gar nicht realisierbar. Falls eine Sortierung vorgenommen werden muss, mit der sich bestimmte Datentypen aus dem Datenfluss aussondern lassen, muss diese entgegen der Bestimmung, die im Vorentwurf vorgesehen war, grundsätzlich durch den Dienst erfolgen. Allein schon aus Fragen der Haftung für die Vollständigkeit der Daten ist es heikler, diese Aufgabe einer anderen Stelle zu übertragen, insbesondere den Fernmeldedienstanbieterinnen. In diesem Zusammenhang geht es beispielsweise darum, im betreffenden Datenfluss die Daten des Fernsehens von jenen des E-Mail-Verkehrs zu trennen. Ein derartiges Ersuchen der anordnenden Behörde erfolgt grundsätzlich nur, wenn diese nicht wünscht, in weitere Daten Einsicht zu nehmen, oder wenn die die erwähnte Trennung des Datenflusses aus technischen Gründen notwendig ist, um die gewünschten Daten aus dem betreffenden Datenfluss korrekt auszuwerten, da die Datenmenge eines Datenflusses so gross sein kann, dass sich die Daten nur schwer oder gar nicht auswerten lassen. Im Hinblick auf die Transparenz, die für eine objektive Beweiswürdigung notwendig ist, muss in den Gerichtsakten

gegebenenfalls vermerkt werden, dass die in den Akten enthaltenen Daten nur einen Teil des gesamten Datenflusses darstellen.

Art. 18 Qualitätskontrolle

Wie die Artikel 32–34 ist *Artikel 18* darauf ausgerichtet, eine ordnungsgemässe Ausführung der angeordneten Überwachungen sicherzustellen.

Absatz 1 soll dem Dienst ermöglichen, Kontrollmassnahmen zu treffen, um ein Qualitätsproblem zu beheben, das allenfalls von der beteiligten Strafverfolgungsbehörde oder von ihm selbst im Zusammenhang mit den Daten festgestellt wird, die von den Fernmeldedienstanbieterinnen geliefert werden. Ein derartiges Problem besteht beispielsweise im folgenden angenommenen Fall: Die Strafverfolgungsbehörde stellt fest, dass die Randdaten, die bei einer rückwirkenden Überwachung beschafft wurden, auf Fernmeldeverkehr hinweisen, der in den Gesprächsaufzeichnungen nicht enthalten ist, die bei einer Echtzeit-Überwachung beschafft wurden. Zudem soll diese Bestimmung dem Dienst ermöglichen, derartige Situationen von vornherein zu verhindern, indem er präventive Kontrollen durchführt, um sich zu vergewissern, dass der reibungslose Ablauf der Überwachungen nicht beeinträchtigt wird. Es versteht sich von selbst, dass der Dienst gestützt auf Artikel 3 Absatz 3 und auch Artikel 5 die betreffende Strafverfolgungsbehörde über etwaige Probleme mit der Datenqualität informiert, denn die Daten können in einem Verfahren ausschlaggebend sein.

Muss der Dienst zur Durchführung der erwähnten Kontrollen vom Inhalt der Daten, die von den Anbieterinnen von Fernmeldediensten geliefert werden, Kenntnis nehmen – was der Fall ist, wenn er Daten aus einer tatsächlichen Überwachung prüfen muss, also echte Daten über ein echtes «Ziel» –, muss er gemäss *Absatz 2* aus Datenschutzgründen vorgängig die Einwilligung der anordnenden Behörde oder der nach ihr mit dem Verfahren befassten Behörde einholen. Der Dienst ist nämlich nicht ohne Weiteres befugt, vom Inhalt der Daten Kenntnis zu nehmen, selbst wenn sich diese in seinem Besitz befinden, da sie in seinem Verarbeitungssystem aufgezeichnet sind. Hingegen ist eine derartige Einwilligung nicht notwendig, wenn der Dienst eine Kontrolle durchführt, ohne von den betreffenden Daten Kenntnis nehmen zu müssen, wie dies bei einer fiktiven Überwachung im Rahmen einer präventiven Kontrolle der Fall ist, also bei einem (fiktiven) «Testziel» und fiktiven Daten.

2.4 4. Abschnitt: Pflichten bei der Überwachung des Postverkehrs

Art. 19 Pflichten der Anbieterinnen von Postdiensten

Artikel 19 ersetzt Artikel 12 des geltenden BÜPF.

Absatz 1 entspricht im Wesentlichen Artikel 12 Absatz 1 des geltenden BÜPF. Die Postsendungen und die Randdaten des Postverkehrs müssen nicht dem Dienst, sondern direkt der anordnenden Behörde (oder der von dieser bezeichneten Behörde) geliefert werden; dies im Unterschied zu den Daten aus der Überwachung des Fernmeldeverkehrs, welche grundsätzlich dem Dienst zu übermitteln sind (siehe Art. 26 Abs. 1). In *Absatz 1* werden zwei allgemeine Überwachungstypen genannt, welche die Daten betreffen und bereits in der Regelung nach dem *geltenden* BÜPF

bestehen: Die Überwachung, die sich auf den Inhalt der Postsendungen bezieht (Inhaltsdaten; *Bst. a*), sowie jene, die sich auf die Randdaten bezieht (*Bst. b*), die keine Rückschlüsse auf den Inhalt der Postsendungen erlauben. Die Definition der Randdaten des Postverkehrs wird gegenüber der heute geltenden Begriffsbestimmung in der unnötigerweise bestimmte Datenkategorien aufgezählt werden, geändert. Der materielle Inhalt des Begriffs bleibt jedoch unverändert. Diese Änderung der Definition hat zur Folge, dass auch die Definitionen in den Artikeln 273 Absatz 1 StPO und 70*d* Absatz 1 MStP geändert werden. Um den Anforderungen des Legalitätsprinzips gerecht zu werden, wird zudem in Anlehnung an den Inhalt von Artikel 11 Buchstabe b der geltenden VÜPF in Absatz 1 festgehalten, dass die betreffenden Postsendungen und die betreffenden Daten nicht mehr nur der anordnenden Behörde, sondern auch der von dieser bezeichneten (Strafverfolgungs-) Behörde geliefert werden können. Insbesondere die Polizei kann die beschafften Postsendungen und Daten erhalten, da sie in der Praxis grundsätzlich sie mit der Auswertung beauftragt wird. Nach Artikel 12 Absatz 1 des geltenden BÜPF sind die Anbieterinnen von Postdiensten verpflichtet, weitere Auskünfte zu erteilen; diese Pflicht wird aufgehoben. Diese Auskünfte hängen nämlich nicht von Kenntnissen der Postdienstanbieterinnen ab, sondern von den Kenntnissen bestimmter Personen wie zum Beispiel denen eines Postboten. Sie müssen somit auf normalem Weg, d.h. über eine Anhörung der betreffenden Person als Zeugen, beschafft werden[39]. Es versteht sich von selbst, dass die Anbieterinnen über die Daten verfügen müssen, damit sie ihrer Pflicht nach Lieferung nachkommen können. Dies bedeutet, dass sie die Randdaten auch aufbewahren müssen. Eine Speicherung der Daten aus der Überwachung des Postverkehrs im Verarbeitungssystem des Dienstes ist nicht vorgesehen.

In *Absatz 2* sind zwei weitere allgemeine Überwachungstypen erwähnt, die bereits nach der Regelung im geltenden BÜPF bestehen. Sie beziehen sich auf den Zeitpunkt, an dem die Überwachungen durchgeführt werden: die Echtzeit-Überwachung und die rückwirkende Überwachung nach Ziffer 3 bzw. 4 des Anhangs zur geltenden VÜPF.

Absatz 3 stellt eine Delegationsnorm dar, mit der dem Bundesrat die Kompetenz erteilt wird, Punkte zu präzisieren, die er bereits heute in der VÜPF regelt. Zurzeit hat der Bundesrat nur die Pflicht festgelegt, die verfügbaren Randdaten zu speichern und zu liefern; solche Daten existieren zum Beispiel im Fall von Postsendungen mit Zustellnachweis, dies im Gegensatz zum einfachen Versand eines Briefes. Es ist darauf hinzuweisen, dass der Entwurf im Bereich Postüberwachung – im Gegensatz zur Überwachung des Fernmeldeverkehrs (siehe Art. 26 Abs. 6) – keine Möglichkeit vorsieht, bestimmte Kategorien von Dienstleistern von bestimmten gesetzlichen Pflichten zu befreien. Dies ist einerseits dadurch gerechtfertigt, dass die Erfüllung der Pflichten gemäss Absatz 1 keine besonderen technischen Schwierigkeiten bereitet (anders als bei den Pflichten der Anbieterinnen von Fernmeldediensten). Andererseits müssen im Bereich Postverkehr nur die oben erwähnten Randdaten gespeichert werden; diese Randdaten fallen zudem nicht bei allen Kategorien von Postsendungen an. Damit sind nicht alle Anbieter von Postdienstleistungen von dieser Aufbewahrungspflicht betroffen. Um zu bestimmen, welche Regelung auf die Überwachung des Verkehrs anwendbar ist, sollte für jeden neu entwickelten Dienst, wie zum Beispiel die elektronischen Postdienste, festgelegt werden, ob er einen

39 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 12 BÜPF N 4.

Postdienst oder einen Fernmeldedienst darstellt. Für neuartige Dienste, die sowohl postalische als auch fernmeldetechnische Merkmale aufweisen, kann eine Anpassung der Ausführungsbestimmungen notwendig sein.

Absatz 4, der von Artikel 12 Absatz 2 des geltenden BÜPF ausgeht, betrifft die Aufbewahrungsfrist für die Randdaten im Bereich des Postverkehrs. Die darin festgelegte Pflicht bedeutet, dass die Anbieterinnen von Postdiensten wie nach der Regelung im geltenden BÜPF die Randdaten zu allen Postsendungen auf «Vorrat» für allfällige künftige Strafuntersuchungen aufbewahren müssen. Welche Randdaten genau aufzubewahren sind, legt der Bundesrat gestützt auf die Kompetenz fest, die ihm in Absatz 3 übertragen wird. Diese Regelung ist notwendig, damit die erwähnten Anbieterinnen die Pflicht erfüllen können, die ihnen nach Absatz 1 Buchstabe b im Fall einer rückwirkenden Überwachung zukommt. Die von dieser Bestimmung erfassten Daten sind zur Bekämpfung der Kriminalität absolut unabdingbar. Die Verlängerung der Aufbewahrungsfrist für die Randdaten im Bereich des Postverkehrs von sechs auf zwölf Monate ist insbesondere im Zusammenhang mit der Motion Schweiger 06.3170 (Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf elektronischen Netzwerken) zu sehen. In dieser Motion wurde unter anderem eine derartige Verlängerung der Aufbewahrungsfrist für die Randdaten im Bereich des Fernmeldeverkehrs, einschliesslich des Internetverkehrs, verlangt (siehe die Erläuterungen zu Art. 26 Abs. 5). Das Problem, auf das sich diese Motion bezieht (der Verlust von für die Strafverfolgung wichtigen Daten), stellt sich praktisch jedoch nicht nur bei den Randdaten im Fernmeldeverkehr, sondern auch im Postverkehr. Somit muss die Verlängerung der Aufbewahrungsfrist logischerweise auch für die Randdaten des Postverkehrs gelten. Siehe im Übrigen sinngemäss die Erläuterungen zu Artikel 26 Absatz 5. Der Bundesrat schätzt den Mehraufwand für die Postdienstleister im Zusammenhang mit der Verlängerung der Aufbewahrungspflicht als vertretbar ein, weil sie die Randdaten bereits heute aufbewahren müssen, diese zudem nicht bei allen Sendungskategorien anfallen und die Speicherung keine besonderen technischen Schwierigkeiten bereitet (siehe Erläuterungen zu Abs. 3). Es gibt deshalb keinen Grund, für die Randdaten des Postverkehrs eine abweichende (kürzere) Aufbewahrungsfrist vorzusehen.

Die Tatsache, dass Postsendungen Gegenstand einer Überwachung bilden, bedeutet nicht zwangsläufig, dass die überwachte Person sie nicht erhalten darf. Auf dieser Idee beruht *Absatz 5*. Die jeweilige Anbieterin von Postdiensten kann diese Sendungen jedoch erst zurückerhalten und sie der überwachten Person zustellen, nachdem die anordnende Behörde oder die nach ihr mit dem Verfahren befasste Behörde ihre Einwilligung erteilt hat. Die Behörde kann selbstverständlich ihre Zustimmung verweigern, wenn die Postsendungen zum Beispiel im Hinblick auf ihre Einziehung oder als Beweismittel beschlagnahmt werden müssen. Ausserdem darf die Anbieterin von Postdiensten der überwachten Person natürlich nicht mitteilen, dass die herausgegebenen Postsendungen, die sie ihr zustellt, Gegenstand einer Überwachung waren. Ein solches Verhalten würde Artikel 39 Absatz 1 Buchstabe d zuwiderlaufen. Eine derartige Mitteilung erfolgt gegebenenfalls im Rahmen und zu den Bedingungen von Artikel 279 StPO.

Art. 20 Informationen vor der Anordnung einer Überwachung

Artikel 20 ist auf die Informationen ausgerichtet, die erforderlich sind, bevor eine Überwachung angeordnet wird. Solche Informationen können insbesondere von Nutzen sein, wenn in Betracht gezogen wird, eine spezielle Überwachung anzuord-

nen, d.h. eine Überwachung, die im Vergleich zu den üblicherweise angeordneten Überwachungen gewisse Besonderheiten aufweist.

2.5 5. Abschnitt: Auskünfte im Zusammenhang mit der Überwachung des Fernmeldeverkehrs

Eine grosse Gruppe von Vernehmlassungsteilnehmern aus fast allen angehörten Kreisen verlangte, dass die Mitwirkungspflichten genauer umschrieben werden, da sie im geltenden Gesetz und im VE-BÜPF zu wenig klar formuliert seien. Für Einzelheiten siehe den Vernehmlassungsbericht[40].

Auch der Bundesrat ist der Auffassung, dass die verschiedenen Mitwirkungs- und Duldungspflichten geklärt werden müssen. Dies erfolgt in den Artikeln 21–25 (5. Abschnitt: Auskünfte im Zusammenhang mit der Überwachung des Fernmeldeverkehrs), in den Artikeln 26–30 (6. Abschnitt: Pflichten bei der Überwachung des Fernmeldeverkehrs) und in den Artikeln 31–34 (7. Abschnitt: Sicherstellung der Auskunfts- und Überwachungsbereitschaft der Anbieterinnen von Fernmeldediensten). Der Umfang der Mitwirkungspflicht wird entsprechend der spezifischen Tätigkeit abgestuft definiert.

Allerdings ist es nicht angebracht, diese Pflichten im Gesetz detailliert festzulegen; die Einzelheiten sollen auf dem Verordnungsweg durch den Bundesrat geregelt werden (VÜPF). Diese Flexibilität ist nicht zuletzt deshalb wichtig, weil die Grenzen zwischen klassischer Fernmeldedienstanbieterin (wie z.B. Swisscom) und dem eher neuen Phänomen der Anbieterin abgeleiteter Kommunikationsdienste (wie z.B. Google) zunehmend verwischen. Der Bundesrat soll daher die Kompetenz erhalten, die Anbieterinnen abgeleiteter Kommunikationsdienste, die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten, verpflichten zu können, alle oder einen Teil der Pflichten zu erfüllen, welche auch die Anbieterinnen von Fernmeldediensten erfüllen müssen (für Einzelheiten siehe die Erläuterungen zu Art. 27 Abs. 3). Entsprechend soll der Bundesrat ebenfalls die Kompetenz erhalten, Anbieterinnen von Fernmeldediensten von bestimmten gesetzlichen Pflichten befreien zu können, insbesondere wenn sie Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten (für Einzelheiten siehe die Erläuterungen zu Art. 26 Abs. 6).

Art. 21 Auskünfte über Fernmeldedienste

Artikel 21 entspricht im Wesentlichen Artikel 14 Absätze 2–4 des geltenden BÜPF und ergänzt ihn. Der Begriff «(Fernmelde-)Dienste» ersetzt den Begriff «(Fernmelde-)Anschlüsse», da sich dieser mit der technischen Entwicklung als zu eng erwiesen hat (siehe Erläuterungen zu Art. 15). Die Internetzugangsanbieterinnen werden durch diese Bestimmung ebenfalls verpflichtet (siehe die Erläuterungen zu Art. 2 Bst. b), und die erfassten Fernmeldedienste umfassen auch die Internetdienste (siehe die Erläuterungen zu Art. 1 Abs. 1). Während sich die Pflicht der Fernmeldedienstanbieterinnen, die entsprechenden Auskünfte zu erteilen, im Bereich der

40 www.admin.ch/ch/d/gg/pc/documents/1719/Bericht_V_Ueberwachung_des_Post-und_Fernmeldeverkehrs.pdf

Mobiltelefonie gegenwärtig auf Prepaid-SIM-Karten und ähnliche Mittel erstreckt, wird sie sich im Internetbereich neu auch auf Prepaid-Wireless-Karten (für den kabellosen Zugang) und ähnliche Mittel beziehen. Diese Ausdehnung wird in der Motion Glanzmann-Hunkeler 07.3627 (Registrierungspflicht bei Wireless-Prepaid-Karten) verlangt. In dieser wird gefordert, die Daten aufzuzeichnen, die bei der Benutzung dieser Mittel eine Teilnehmeridentifikation ermöglichen, wie dies zurzeit bei den Prepaid-SIM-Karten der Fall ist. Damit soll insbesondere verhindert werden, dass im Internet anonym Bilder oder Videos mit pädophilen Darstellungen heruntergeladen werden können. Diese Pflicht gilt ausserdem für Mittel, die den Zugang zum Festnetz ermöglichen.

Im Gegensatz zum Inhalt des Fernmeldeverkehrs und zu den Randdaten unterstehen die in *Artikel 21* erwähnten Auskünfte nicht dem Fernmeldegeheimnis; diese Auskünfte können somit im Rahmen eines vereinfachten Verfahrens erteilt werden[41], wie dies nach der Regelung im geltenden BÜPF der Fall ist, und deren Beschaffung stellt keine Zwangsmassnahme dar. Die Auskunftserteilung muss somit nicht im Rahmen eines Verfahrens erfolgen, das den Beschränkungen von Artikel 269 StPO unterliegt, insbesondere der Liste der Straftaten, die in Absatz 2 dieses Artikels enthalten ist[42], und erfordert keine Genehmigung durch die Genehmigungsbehörde (Art. 274 StPO). Diese Auskünfte sind äusserst wichtig für den Fortgang der Ermittlungen[43], die aufgrund der erzielten Ergebnisse zur Anordnung einer Überwachung nach den strengen Bedingungen von Artikel 269 StPO führen können. Damit die betreffenden Personen ihrer Pflicht, die Angaben und Erteilung von Auskünften nach *Artikel 21* zu liefern, nachkommen können, müssen sie selbstverständlich über die erforderlichen Angaben und Auskünfte verfügen . Dies bedeutet, dass die betreffenden Personen diese Angaben und Auskünfte aufbewahren müssen. Die Personen, denen die Auskünfte erteilt werden müssen, sind in Artikel 15 genannt. Gestützt auf Artikel 15 Absatz 1 Buchstaben a und b können die Auskünfte direkt der Polizei erteilt werden, ohne dass die Staatsanwaltschaft im Fall von Artikel 15 Absatz 1 Buchstabe b eine Anordnung erlassen muss (für Einzelheiten, siehe die Erläuterungen zu diesen Bestimmungen).

Die Auskünfte nach *Absatz 1* Buchstabe a–d müssen von den Fernmeldedienstanbieterinnen auch dann erteilt werden, wenn sie in keinem Abonnementsverhältnis zum Kunden stehen (siehe Abs. 2); falls kein Abonnementsverhältnis besteht, sind zudem die Angaben nach Abs. 1 Bst. e zu erfassen. Die Modalitäten für die Erfassung der Angaben nach Absatz 1 Buchstabe a werden vom Bundesrat bestimmt (für Einzelheiten siehe die Erläuterungen zu Art. 23). Die Anbieterinnen von Fernmeldediensten sind somit in der Lage, die Auskünfte nach *Absatz 1* mittels des Systems zur Vermittlung der Auskunftsgesuche über die Fernmeldedienste (gegenwärtig CCIS genannt) zu erteilen, das der Dienst in Zusammenarbeit mit ihnen führt. Zu den korrespondierenden Pflichten der Wiederverkäufer von Mitteln wie z.B. Prepaid-Karten siehe Artikel 30.

Absatz 1 Buchstabe a entspricht Artikel 14 Absatz 1 Buchstabe a des geltenden BÜPF, wobei zusätzlich der Name und das Geburtsdatum aufgeführt werden. Diese beiden klassischen Identifikationsmerkmale sind für die Behörden und im Hinblick auf die in Artikel 15 aufgeführten Zwecke sehr wichtig.

41 Vgl. Botschaft vom 1. Juli 1998 zum geltenden BÜPF, BBl **1998** 4278.
42 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 14 BÜPF N 1–4, 23.
43 Vgl. Botschaft vom 1. Juli 1998 zum geltenden BÜPF, BBl **1998** 4278.

Absatz 1 Buchstabe b entspricht im Wesentlichen Artikel 14 Absatz 1 Buchstabe b des geltenden BÜPF. Da Artikel 3 Buchstabe f FMG den Begriff der «Kommunikationsparameter» enthält, der in Artikel 3 Buchstabe g FMG definiert ist, wird der Verweis in *Buchstabe b* aus Gründen der Klarheit entsprechend ergänzt.

Absatz 1 Buchstabe c lehnt sich an Artikel 14 Absatz 1 Buchstabe c des geltenden BÜPF an, wobei die Mehrzahl verwendet wird. Wenn die Überwachung einer Person gewünscht wird, ist es sinnvoll, dass alle Dienste (zum Beispiel Festnetz, Mobiltelefon und Internet), welche diese Person benutzt, bekannt sind und. Damit lässt sich bestimmen, welche Dienstarten überwacht werden müssen. Zudem kann dadurch vermieden werden, dass die Anbieterinnen von Fernmeldediensten mehrmals kontaktiert werden müssen, wenn die fragliche Person über verschiedene Dienstarten verfügt.

Aufgrund der in *Absatz 1 Buchstabe d* vorgesehenen Delegationsnorm erhält der Bundesrat die Kompetenz, die Anbieterinnen von Fernmeldediensten zu verpflichten, dem Dienst weitere geeignete Auskünfte über die Fernmeldedienste zu erteilen, beispielsweise den Zeitpunkt der Einschaltung des Dienstes, den Status des Dienstes (zum Beispiel aktiv, gesperrt oder gekündigt), die PUK-Nummer, die SIM-, IMEI- und IMSI-Nummer, die Rechnungen, die Zahlungsmodalitäten und die Verträge. Auf Grundlage dieser Bestimmung können sie auch verpflichtet werden, andere nützliche Daten als jene nach Buchstabe a zu liefern, mit welchen die Person ebenfalls identifiziert werden kann, beispielsweise eine Kopie des vorgelegten Personalausweises. So kann der Bundesrat zum Beispiel vorsehen, dass die Registrierung nur gegen Vorlage eines Passes, einer gültigen Identitätskarte oder eines anderen Reisepapiers erfolgen darf, das zur Einreise in die Schweiz oder zum dortigen Aufenthalt berechtigt, dass die Art und Nummer des Ausweispapiers erfasst werden müssen und dass zudem eine Kopie des vorgelegten Ausweises erstellt werden muss. Einige dieser Auskünfte sind gegenwärtig in den Weisungen des Dienstes genannt und können somit von den Strafverfolgungsbehörden bereits beschafft werden. Es ist sehr wahrscheinlich, dass der Bundesrat zumindest diese Auskünfte in der Verordnung übernimmt. Die vom Bundesrat gestützt auf *Absatz 1 Buchstabe d* vorgeschlagenen Bestimmungen werden den betroffenen Kreisen in einer Vernehmlassung bzw. Anhörung unterbreitet. Sofern der Bundesrat es vorsieht (siehe Abs. 5), können die betreffenden Auskünfte gestützt auf Artikel 15 Absatz 1 Buchstaben a und b (für weitere Einzelheiten, siehe die Erläuterungen zu diesen Bestimmungen) über ein System zur Vermittlung der Auskunftsgesuche über die Fernmeldedienste (aktuell CCIS genannt) auch direkt der Polizei erteilt werden, ohne dass die Staatsanwaltschaft in Fällen nach Artikel 15 Absatz 1 Buchstabe b eine Anordnung erlassen muss. Da es sich bei diesen Daten nicht um besonders schützenswerte Personendaten im Sinne von Artikel 3 Buchstabe c DSG handelt, ist es nicht notwendig, ihre Bearbeitung in einem Gesetz im formellen Sinn wie dem BÜPF vorzusehen (Art. 17 DSG). Der vorliegende Gesetzesentwurf muss keine Bestimmung enthalten, in der die Arten dieser Auskünfte aufgezählt werden, denn eine solche Bestimmung wäre zu detailliert, um in ein Gesetz im formellen Sinn aufgenommen zu werden. Die Aufzählung ist in einer Verordnung einzufügen.

Absatz 1 Buchstabe e sieht vor, dass die Anbieterinnen von Fernmeldediensten in der Lage sein müssen, die folgenden Angaben zu machen: Den Namen und Vornamen der Person, die das für den Zugang zum Dienst erforderliche Mittel (Prepaid-SIM-Karte oder ähnliches Mittel, Prepaid-Wireless-Karte oder ähnliches Mittel und Mittel für den Zugang zum Festnetz) gegen Entgelt oder kostenlos abgegeben hat,

sowie die Stelle, an der es abgegeben wurde. Diese Pflicht ist notwendig, damit klar ist, wem ein allfälliges Versäumnis bei der Aufzeichnung der Daten nach Absatz 1 Buchstabe a–d zur Last zu legen ist. Zu den korrespondierenden Pflichten der Wiederverkäufer von solchen Mitteln siehe Artikel 30.

Absatz 2 regelt die Pflicht zur Erfassung und zur Verfügbarkeit der in Absatz 1 aufgeführten Angaben; dabei ist es unerheblich, ob die Kundenbeziehung über ein Abonnementsverhältnis geführt wird oder nicht. Der Regelungsgehalt von Absatz 2 ist teilweise aus Artikel 15 Absatz 5bis des geltenden BÜPF übernommen worden und passt diesen an. Die Pflicht der Fernmeldedienstanbieterinnen, die entsprechenden Auskünfte zu erteilen, wird ausgedehnt. Während sich diese Pflicht im Bereich der Mobiltelefonie gegenwärtig auf Prepaid-SIM-Karten und ähnliche Mittel erstreckt, wird sie sich im Internetbereich neu auch auf Prepaid-Wireless-Karten (für den kabellosen Zugang) und ähnliche Mittel beziehen. Diese Ausdehnung hängt mit den Forderungen zusammen, die in der Motion 07.3627 Glanzmann-Hunkeler gestellt werden. Konsequenterweise sind nunmehr auch Mittel erfasst, die ohne Abschluss eines Abonnements den Zugang zum Festnetz ermöglichen, denn es hatte sich im Rahmen der Terrorismusbekämpfung im Zusammenhang mit den Prepaid-SIM-Karten gezeigt , dass die erwähnten Auskünfte auch zu einer Kundenbeziehung, die nicht über ein Abonnementsverhältnis aufgenommen wurde, zur Verfügung stehen müssen. Im geltenden BÜPF ist eine Frist von zwei Jahren nach der Aufnahme der Kundenbeziehung vorgesehen, in der es möglich sein muss, die fraglichen Auskünfte zu erteilen. Diese zweijährige Frist war festgelegt worden, weil zum Zeitpunkt des Inkrafttretens von Artikel 15 Absatz 5bis des geltenden BÜPF, d.h. am 1. August 2004, entschieden worden war, es ginge zu weit, die rückwirkende Aufzeichnung der vor dem 1. August 2002 gekauften Prepaid-SIM-Karten zu verlangen[44]. Da unterdessen keine rückwirkende Aufzeichnung mehr notwendig ist, kann diese Frist aufgehoben werden. Diese Aufhebung erfordert, dass eine Übergangsbestimmung vorgesehen wird, die auf Prepaid-SIM-Karten und ähnliche Mittel anwendbar ist (Art. 45 Abs. 4). Zudem ist darauf hinzuweisen, dass sich die erwähnte Auskunftspflicht nur auf jene Auskünfte bezieht, die bei der Registrierung aufgezeichnet werden, die eine Fernmeldedienstanbieterin bei der Aufnahme einer Kundenbeziehung vornehmen muss (Erstregistrierung) und bei der sie Prepaid-SIM-Karten (oder ähnlichen Mitteln), Prepaid-Wireless-Karten (oder ähnlichen Mitteln) oder Mitteln für den Zugang zum Festnetz abgibt. Nicht von dieser Auskunftspflicht betroffen sind hingegen die Daten zu Personen, die diese Mittel in der Folge kaufen könnten. Dies bedeutet, dass die Anbieterinnen von Fernmeldediensten nur in der Lage sein müssen, jene Auskünfte zu erteilen, die sie bei der Erstregistrierung verlangen mussten; dies unter Ausschluss von Daten allfälliger künftiger Käuferinnen und Käufer der Mittel. Das gegenteilige Vorgehen wäre mit übertriebenen Formalitäten und einem unverhältnismässigen administrativen Aufwand verbunden (siehe auch die Erläuterungen zu Art. 6*a* FMG).

Es ist zu beachten, dass *Absatz 2* den Anwendungsbereich von Artikel 22 nicht einschränkt.

Die Verletzung der Registrierungspflichten wird nach Artikel 39 Absatz 1 Buchstabe c geahndet.

44 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 15 BÜPF N 22.

Art. 22 Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet

Artikel 22 wird im Wesentlichen aus Artikel 14 Absatz 4 des geltenden BÜPF übernommen und sieht eine Mitwirkungspflicht der Anbieterinnen von Fernmeldediensten vor. Diese müssen alles in ihrer Macht stehende unternehmen, um die Identifikation zu ermöglichen. Aus diesem Artikel lässt sich jedoch keine Pflicht für die Anbieterinnen von Fernmeldediensten ableiten, den Namen der Person anzugeben, die einen Computer tatsächlich benutzt, da dies nicht in ihrer Macht steht. Hingegen müssen sie beispielsweise – soweit sie der Bundesrat dazu verpflichtet – den Namen der Person angeben, der die betreffende IP-Adresse zugewiesen wurde. Wie dies nach dem geltenden BÜPF der Fall ist, kann die Mitteilung der Angaben gemäss *Artikel 22* in einem vereinfachten Verfahren erfolgen (siehe dazu die Erläuterungen zu Art. 21).

Artikel 22 ist auf die Identifikation der Täterschaft bei Straftaten über das Internet ausgerichtet; *Absatz 1* umfasst deshalb alle Angaben, die eine solche Identifikation ermöglichen[45]. Mit dem Ziel der Identifikation können Randdaten, zum Beispiel die Zuordnung einer dynamischen (d.h. nicht im Voraus zugeteilten) IP-Adresse, nach dem vereinfachten Verfahren beschafft werden[46]. Das BÜPF überträgt dem Dienst die Rolle einer Schnittstelle. Aus Kohärenzgründen wird daher festgehalten, dass die Angaben dem Dienst und nicht wie im geltenden Recht der zuständigen Behörde zu liefern sind[47].

Artikel 14 Absatz 4 des geltenden BÜPF ist allgemein gehalten. Im Gegensatz dazu enthält *Absatz 2* eine Delegationsnorm, die den Bundesrat ausdrücklich beauftragt, nach dem Modell von Artikel 27 der geltenden VÜPF anzugeben, welche Daten die Anbieterinnen von Fernmeldediensten liefern müssen. Die vom Bundesrat gestützt auf *Absatz 2* vorgeschlagenen Bestimmungen werden den betroffenen Kreisen in einer Vernehmlassung bzw. Anhörung unterbreitet.

Auch die Personen nach Artikel 2 Buchstaben c und d verfügen über Angaben, die im Kontext, auf den sich Artikel 22 bezieht, von Nutzen sein können. *Absatz 3* verlangt von ihnen jedoch nur, dass sie als Folge der Artikel 27 Absatz 2 und 28 Absatz 2 die ihnen vorliegenden Angaben mitteilen müssen (zumindest jene, die ihnen zum Zeitpunkt des Gesuchs zur Verfügung stehen).

Der Bundesrat kann allerdings zum Schluss gelangen, dass diese Regelung für eine effiziente Identifikation von Internet-Straftätern nicht ausreicht. Deshalb ermöglicht ihm die Delegationsnorm in *Absatz 4*, die Personen nach Artikel 2 Buchstabe c unter ganz bestimmten Bedingungen (siehe sinngemäss die Erläuterungen zu Art. 27 Abs. 3) als Folge von Artikel 27 Absatz 3 zu verpflichten, zusätzliche Angaben zu liefern. Als Modell dienen dabei die Angaben, die von den Fernmeldedienstanbieterinnen geliefert werden müssen.

Art. 23 Modalitäten der Datenerfassung und der Auskunftserteilung

Nach *Absatz 1* werden die Modalitäten für die Aufzeichnung der Daten nach Artikel 21 Absatz 1 Buchstabe a und Artikel 22 Absatz 2 Satz 1 vom Bundesrat bestimmt. Dieser kann zum Beispiel vorsehen, dass die Registrierung für einen

45 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 14 BÜPF N 25.
46 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 14 BÜPF N 26.
47 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 14 BÜPF N 24.

Fernmeldedienst nur gegen Vorlage eines Passes, einer gültigen Identitätskarte oder eines anderen Reisepapiers erfolgen darf, das zur Einreise in die Schweiz oder zum dortigen Aufenthalt berechtigt, dass die Art und Nummer des Ausweispapiers erfasst werden müssen und dass zudem eine Kopie des vorgelegten Ausweises erstellt werden muss.

Absatz 2 wird aus Artikel 14 Absatz 3 erster Satz des geltenden BÜPF übernommen.

Unter dem geltenden BÜPF hatte sich der Bundesrat entschieden, die in Artikel 21 Absatz 1 genannten Daten den Behörden nach Artikel 15 wenn möglich durch ein Abrufverfahren mittels eines Systems zur Vermittlung der Auskunftsgesuche über die Fernmeldeanschlüsse (CCIS genannt) zugänglich zu machen, das vom Dienst in Zusammenarbeit mit den Fernmeldedienstanbieterinnen erstellt und geführt wird (Art. 19 ff. der geltenden VÜPF). Für Auskünfte, die nicht auf diese Weise abgerufen werden können, wird (grundsätzlich per Fax) ein Gesuch an den Dienst gerichtet, der dieses an die Fernmeldedienstanbieterinnen weiterleitet. Der Bundesrat hatte somit nicht vorgesehen, den Behörden nach Artikel 15 zu ermöglichen, direkt auf die bestehenden, nicht öffentlich zugänglichen Verzeichnisse zuzugreifen. Mit *Absatz 3* erhält der Bundesrat die Möglichkeit, das aktuelle System zu ändern. Wenn er es als angezeigt erachtet, kann er z.B. vorsehen, dass die Daten nach den Artikeln 21 und 22 durch einen Online-Zugriff auf das System zur Vermittlung der Auskunftsgesuche über die Fernmeldedienste zugänglich gemacht werden. Dabei ist zu erwähnen, dass die Polizeidienste nach Artikel 15 Absatz 1 Buchstabe b von sich aus beim Dienst die Auskünfte nach Artikel 21 und 22 verlangen und von diesem erhalten können und dafür keine Anordnung des Staatsanwaltschaft brauchen (für Einzelheiten, siehe die Erläuterungen zu Art. 15 Abs. 1 Bst. b).

Art. 24 Informationen vor der Anordnung einer Überwachung

Im Gegensatz zum Fall, der in Artikel 26 Absatz 2 vorliegt, ist Artikel 24 darauf ausgerichtet, Informationen (zum Beispiel über den Standort einer Mobilfunkantenne) zu erhalten, bevor eine Überwachung angeordnet wird. Solche Informationen können insbesondere von Nutzen sein, wenn in Betracht gezogen wird, eine spezielle Überwachung anzuordnen, d.h. eine Überwachung, die im Vergleich zu den üblicherweise angeordneten Überwachungen gewisse Besonderheiten aufweist.

Art. 25 Informationen über Dienstleistungen

Wie die Artikel 32–34 soll *Artikel 25* sicherstellen, dass die angeordneten Überwachungen korrekt ausgeführt werden können, insbesondere dass die Überwachung keine Lücken aufweist. Dabei geht es insbesondere darum, dass der Dienst die Schwierigkeiten voraussehen kann, die im Rahmen von künftigen Überwachungen auftreten könnten, und sich nicht darauf beschränken muss, auf Probleme zu reagieren, die sich unter Umständen bei der Durchführung dieser Überwachungen ergeben. Diesbezüglich ist festzuhalten, dass *Artikel 25* nur vorsieht, dass der Dienst über die Art und die Merkmale der jeweiligen Dienstleistungen informiert wird, nicht jedoch über die Merkmale der Technologie, auf der diese beruhen, denn es ist nicht notwendig, die Merkmale dieser bestimmten Technologie zu kennen. Wichtig ist vielmehr, dass die angeordneten Überwachungen so ausgeführt werden können, wie es die Artikel 18 und 32–34 sicherstellen sollen. In der Praxis müssen die Anbieterinnen von Fernmeldediensten dem Dienst auf Verlangen genau darlegen, um welche Dienstleistungen es sich handelt und worin diese bestehen, d.h. wozu sie dienen.

Dabei ist es unerheblich, ob die fragliche Dienstleistung von einer anderen Person als der Fernmeldedienstanbieterin entwickelt wurde oder ob eine Technologie eingesetzt wird, die von einer Drittperson entwickelt worden ist. Das beratende Organ nach Artikel 5 ist für den Dienst ein geeigneter Rahmen zur Beschaffung solcher Informationen. Es erscheint also nicht nötig, die Anbieterinnen von Fernmeldediensten dazu zu verpflichten, den Dienst von sich aus zu informieren, ohne von diesem angefragt worden zu sein.

In diesem Zusammenhang erhalten Mitarbeiterinnen und Mitarbeiter des Dienstes unter Umständen Kenntnis von Geschäftsgeheimnissen der Fernmeldedienstanbieterinnen. Diesbezüglich ist jedoch festzuhalten, dass diese Mitarbeiterinnen und Mitarbeiter dem Amtsgeheimnis unterstehen. Eine Offenbarung solcher Geheimnisse würde somit unter den Straftatbestand der Verletzung des Amtsgeheimnisses fallen (Art. 320 StGB).

Mit der Frist von sechs Monaten, die in *Artikel 25* genannt wird, soll verhindert werden, dass die Anbieterinnen von Fernmeldediensten dem Dienst die Informationen in einem Stadium liefern müssen, in dem sie sich möglicherweise noch nicht im Klaren sind, ob sie die betreffende Dienstleistung auf den Markt bringen werden – dies trotz der Tatsache, dass die Anbieterinnen ihr Budget in der Regel zwölf Monate im Voraus planen und bei der Einführung eines neuen Überwachungssystems grundsätzlich eine Übergangsfrist von zwölf Monaten wünschen. Die Frist von sechs Monaten soll somit nicht nur den Anbieterinnen von Fernmeldediensten, sondern auch dem Dienst unnötige Arbeit ersparen. Es ist allerdings möglich, dass der Dienst zur Einleitung der erforderlichen Schritte für die korrekte Durchführung der Überwachungen je nachdem mehr Zeit benötigt. Trotzdem wird auf eine Frist von mehr als sechs Monaten verzichtet, denn dies wäre für die Fernmeldedienstanbieterinnen zu langfristig. In der Zwischenzeit müsste also mit Lücken in der Überwachung gerechnet werden. Die hier vorgeschlagene Regelung hindert die Anbieterinnen selbstverständlich nicht daran, ihre ursprüngliche Planung zur Einführung neuer Dienstleistungen zu ändern und anzupassen; eine andere Lösung würde darauf hinauslaufen, dass die Anbieterinnen daran gehindert würden, sich auf dem ausserordentlich dynamischen Telekommunikationsmarkt zu behaupten.

2.6 6. Abschnitt: Pflichten bei der Überwachung des Fernmeldeverkehrs

Für die allgemeinen Bemerkungen zu den Auskunfts- und Überwachungspflichten und zu den Ergebnissen des Vernehmlassungsverfahrens siehe die einleitenden Erläuterungen zum 5. Abschnitt.

Art. 26 Pflichten der Anbieterinnen von Fernmeldediensten

Artikel 26 ersetzt Artikel 15 des geltenden BÜPF, der sich auf die Pflichten der Anbieterinnen bezieht. Er entspricht insbesondere einem berechtigten Wunsch, der im Vernehmlassungsverfahren geäussert worden war: In diesem Rahmen wurde verlangt, die Mitwirkungspflichten namentlich der Anbieterinnen von Fernmeldediensten genauer zu umschreiben, da diese Pflichten im geltenden Gesetz und im VE-BÜPF zu wenig klar formuliert seien. Für Einzelheiten siehe den Vernehmlas-

sungsbericht[48]. Zudem werden im vorliegenden Entwurf die spezifischen Aufgaben aufgehoben, die den Anbieterinnen von Fernmeldediensten im VE-BÜPF im Zusammenhang mit dem Einsatz von Government Software (GovWare) übertragen worden waren. Eine eingehende Analyse hat nämlich gezeigt, dass eine Unterstützung oder ein spezifisches Mitwirken der Fernmeldedienstanbieterinnen nicht notwendig ist, um den Strafverfolgungsbehörden den Einsatz von GovWare zu ermöglichen (siehe auch die Erläuterungen zu Art. 280 Bst. d StPO).

In *Absatz 1* werden zwei allgemeine Überwachungstypen genannt, welche die Daten betreffen und bereits im geltenden BÜPF bestehen. Es handelt sich um die Überwachung, die sich auf den Inhalt des ein- und ausgehenden Fernmeldeverkehrs bezieht (Inhaltsdaten; *Bst. a*), sowie um jene, die sich nur auf die Randdaten des Verkehrs bezieht (*Bst. b*). Anhand der letzteren ist es nicht möglich, vom Inhalt des betreffenden Fernmeldeverkehrs Kenntnis zu nehmen. Wie aus Artikel 8 Buchstabe b hervorgeht, wurde die Definition der Randdaten gegenüber der geltenden Definition vereinfacht, ohne dass sich der materielle Inhalt des Begriffs ändert. So wurde die Erwähnung der «Verkehrs- und Rechnungsdaten» aufgehoben, da diese Datenkategorie durch die neu vorgeschlagene Definition des Begriffs der Randdaten abgedeckt wird. Die Ausdrücke «überwachte Person» und «Daten, aus denen hervorgeht, mit wem» sind im Grunde in der Praxis weniger auf Personen als auf den von diesen benutzten Dienst (z.B. den Anschluss) ausgerichtet. Denn überwacht wird letztlich z.B. der Anschluss der überwachten Person (die auch unbekannt sein kann), der mit einem anderen Anschluss in Verbindung stehen kann. Dieser andere Anschluss ist einer bestimmten Person zugeteilt, bei der es sich nicht zwangsläufig um jene handelt, die diesen anderen Anschluss im betreffenden Zeitpunkt verwendet hat oder verwendet. Diese Änderung der Definition der Randdaten hat zur Folge, dass auch die Definitionen in den Artikeln 273 Absatz 1 StPO und 70*d* Absatz 1 MStP geändert werden. *Absatz 1* deckt selbstverständlich auch die Daten ab, welche die Internetzugänge betreffen, da der Zugang zum Internet eine Art des Fernmeldeverkehrs darstellt (siehe die Erläuterungen zu Art. 1 Abs. 1). Unter die Formulierung von *Absatz 1* fallen insbesondere auch der Inhalt einer SMS (*Bst. a*), die Randdaten einer SMS (*Bst. b*) sowie die blossen Versuche zum Aufbau einer Verbindung (zum Beispiel der Fall, dass die Person, welche die überwachte Person zu erreichen versucht, nicht abhebt; *Bst. b*). Es versteht sich von selbst, dass die betreffenden Personen über die Daten verfügen müssen, damit sie ihrer Pflicht zur Lieferung derselben nachkommen können. Dies bedeutet, dass sie die Randdaten aufbewahren müssen. Für nähere Erläuterungen zum Begriff der Randdaten siehe die Erläuterungen zu Absatz 5. Mit dem Verweis auf Artikel 17 Buchstabe c wird daran erinnert, dass bei einer Überwachung in Form einer Direktschaltung die beschafften Daten ausnahmsweise direkt der anordnenden Behörde oder der von dieser bezeichneten Behörde (im Prinzip einer Strafverfolgungsbehörde) übermittelt werden; sie werden nicht zuerst dem Dienst zugeleitet, der normalerweise als Mittler fungiert. Es ist Sache des Bundesrates zu bestimmen, innerhalb welcher Frist der Erhalt der Daten von den Fernmeldedienstanbieterinnen verlangt werden kann. Die Fernmeldedienstanbieterinnen müssen die von der anordnenden Behörde verlangten Daten liefern. Sofern diese dies wünscht und sofern es im konkreten Fall für sie zumutbar ist, müssen sie also eine Sortierung vornehmen, um aus dem Datenfluss die Daten des gewünschten Datentyps auszusondern (z.B. Internetdaten, mit Ausnahme von

48 www.admin.ch/ch/d/gg/pc/documents/1719/Bericht_V_Ueberwachung_des_Post-und_Fernmeldeverkehrs.pdf

Internetfernsehen). Für weitere Einzelheiten, siehe die Erläuterungen zu Artikel 17 Buchstabe f.

In *Absatz 2* werden Pflichten übernommen, die schon im geltenden BÜPF bestehen (Art. 15 Abs. 1 Satz 2 und Abs. 4 Satz 2) und die für die Durchführung der Überwachung notwendig sind. Im Gegensatz zu Artikel 24 geht es hier um jene Informationen, die erforderlich sind, wenn eine Überwachung bereits angeordnet wurde. Unter diese Bestimmung fallen insbesondere Informationen, die sich auf die verwendete Kommunikationstechnik und die von einzelnen Personen benutzten Geräte beziehen[49]. Mit *Absatz 2* soll bis zu einem gewissen Grad die Lücke in der Überwachung geschlossen werden, die sich aus Absatz 6 ergibt. Dazu werden den erfassten Personen die Minimalpflicht, eine Überwachung zu dulden, sowie die notwendigen Nebenpflichten auferlegt, um die Durchführung dieser Überwachung zu ermöglichen. In Anlehnung an die im heutigen BÜPF geltende Regelung zur Überwachung in einem internen Netzwerk oder einer Hauszentrale wird vorgesehen, dass der Dienst oder eine von ihm beauftragte Person, insbesondere die Polizei, die Überwachung ausführen. Dies bedeutet nicht, dass der Dienst im Sinne von Artikel 178 Absatz 3 der Bundesverfassung (BV)[50] Verwaltungsaufgaben an Private übertragen kann. Der Dienst ist weiterhin für die Durchführung der betreffenden Aufgabe verantwortlich. Zur Herausgabepflicht von nach Absatz 6 dispensierten Anbieterinnen bei Randdaten vgl. die Erläuterungen ebenda.

In *Absatz 3*, der in Verbindung mit Artikel 17 Buchstabe a zu betrachten ist, wird ebenfalls eine Pflicht übernommen, die schon im geltenden BÜPF besteht (Art. 15 Abs. 2 Satz 2) und die für die Durchführung der Überwachung notwendig ist. Auf Verlangen der Behörde, welche die vom Dienst weitergeleitete Überwachungsanordnung erlassen hat, können die Daten vor allem aus Gründen der Vertraulichkeit auch direkt an den Dienst geliefert werden.

In *Absatz 4* sind – neben jenen in Absatz 1 – zwei weitere allgemeine Überwachungstypen erwähnt, die bereits nach der Regelung im geltenden BÜPF bestehen. Sie beziehen sich auf den Zeitpunkt, an dem die Überwachungen durchgeführt werden: die Echtzeit-Überwachung und die rückwirkende Überwachung, die in den Ziffern 3 und 4 des Anhangs der geltenden VÜPF definiert sind. Die im Rahmen einer rückwirkenden Überwachung gesammelten Randdaten werden in der Fachsprache als aufbewahrte Daten («retained data») bezeichnet.

Die in *Absatz 5* festgelegte Pflicht bedeutet, dass die Anbieterinnen von Fernmeldediensten wie nach der heutigen Regelung (Art. 15 Abs. 3) die Randdaten zum gesamten Fernmeldeverkehr auf «Vorrat» für allfällige künftige Strafuntersuchungen aufbewahren müssen. Gestützt auf die Kompetenz, die ihm in Artikel 31 übertragen wird, bezeichnet der Bundesrat die Randdaten, welche aufzubewahren sind. Dies erfordert natürlich, dass die Daten zum Fernmeldeverkehr aller Personen aufbewahrt werden müssen, gegen die während der Aufbewahrungsfrist keine Ermittlung eingeleitet wird; dabei handelt es sich um die überwiegende Mehrheit der Bevölkerung. Diese Regelung ist jedoch notwendig, damit die Anbieterinnen von Fernmeldediensten die Pflicht erfüllen können, die ihnen nach Absatz 1 Buchstabe b im Rahmen einer rückwirkenden Überwachung zukommt. Die von dieser Bestimmung erfassten Daten sind zur Bekämpfung der Kriminalität absolut unabdingbar. Im Gegensatz zu den Daten nach Absatz 1 Buchstabe a (sogenannte Inhaltsdaten)

49 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 15 BÜPF N 5.
50 SR **101**

bieten diese Daten im Übrigen keine Informationen zum Inhalt des Fernmeldeverkehrs. Sie dürfen nicht präventiv, sondern nur im Rahmen eines Strafverfahrens unter Einhaltung der Artikel 269 ff. StPO beschafft werden, d.h. insbesondere mit der Genehmigung der Genehmigungsbehörde (Zwangsmassnahmengericht). Diese starke gesetzliche Garantie schützt alle betroffenen Personen vor allfälligen Missbräuchen. Zudem können alle betroffenen Personen Beschwerde gegen eine angeordnete Überwachung einlegen (Art. 279 StPO). Nebenbei ist anzumerken, dass die Anbieterinnen von Fernmeldediensten bereits heute alle oder einen Teil der betreffenden Daten während mindestens einem Jahr aufbewahren, vor allem aus geschäftlichen Gründen und zum Zweck der Rechnungsstellung.

In *Absatz 5* ist die Frist für die Aufbewahrung der Randdaten festgelegt, die von sechs auf zwölf Monate ab dem Zeitpunkt der Kommunikation verlängert wird. Diese Verlängerung wird in Ziffer 2 der Motion Schweiger 06.3170 (Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf elektronischen Netzwerken) und in der Motion Barthassat 10.4133 (Verlängerung der Aufbewahrungspflicht für Protokolle über die Zuteilung von IP-Adressen) verlangt. Zu den Randdaten des Fernmeldeverkehrs gehören namentlich jene, denen sich die Zuweisung der IP-Adressen entnehmen lässt und auf welche die erwähnte Motion Barthassat ausgerichtet ist. Die Gründe für diese Verlängerung hängen mit der Wirksamkeit der Strafverfolgung zusammen, insbesondere im Bereich der Bekämpfung der Kinderpornografie, des organisierten Verbrechens und des Terrorismus. Die Erfahrungen der Strafverfolgungsbehörden haben gezeigt, dass der Zeitraum, in dem die Randdaten zurzeit aufbewahrt werden müssen, d.h. sechs Monate, zu kurz bemessen ist. Oft ist diese Frist bereits vollständig oder grösstenteils abgelaufen, wenn die Behörde aufgrund des Stands des Verfahrens in der Lage ist, eine Überwachung anzuordnen. Dies kann namentlich zur Folge haben, dass einem internationalen Rechtshilfeersuchen nicht stattgegeben werden kann oder dass eine beschuldigte Person oder, noch schlimmer, ein Opfer, zum Beispiel ein Kind, an dem pädophile Handlungen vorgenommen werden, nicht identifiziert werden kann. Angesichts der öffentlichen Interessen, die auf dem Spiel stehen, ist die Verlängerung der Aufbewahrungsfrist für die betreffenden Daten von sechs auf zwölf Monate mit den Grundrechten der Personen vereinbar, deren Daten aufbewahrt werden. Diesen Standpunkt hat der Bundesrat bereits in seinem Bericht vom 9. Juni 2006 vertreten, der in Erfüllung des Postulats vom 21. Februar 2005 der Sicherheitspolitischen Kommission des Ständerates 05.3006 (Effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen) erstellt wurde[51]. Diese Frist muss insbesondere in Verbindung mit der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 betrachtet werden. In dieser Richtlinie ist für die Daten, die in der Schweiz den Randdaten entsprechen, eine Aufbewahrungsdauer von mindestens sechs Monaten und grundsätzlich höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation vorgesehen[52]. Die Verlängerung der fraglichen Aufbewahrungsfrist stiess im Vernehmlassungsverfahren auf breite Zustimmung. Vor allem in den Kreisen der Fernmeldedienstanbieterinnen wird sie jedoch in Frage gestellt. Diese führen die zusätzlichen Kosten an, die ihnen entstehen. Aus Sicht des Bundesrates verursacht die geplante Verlängerung der Aufbewahrungsfrist jedoch keine unverhältnismässigen Kosten für die Personen, die diese Aufbewahrungspflicht erfüllen müssen. Es ist

51 www.admin.ch/ch/d/ff/2006/5693.pdf
52 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF

zudem daran zu erinnern, dass die Anbieterinnen von Fernmeldediensten schon heute alle oder einen Teil der betreffenden Daten während mindestens einem Jahr aufbewahren. Die Ausdehnung der Frist, für die rückwirkend Randdaten angefordert werden können, von sechs auf zwölf Monate (Art. 273 Abs. 3 StPO und Art. 70*d* Abs. 3 MStP), folgt aus der Verlängerung der Aufbewahrungsfrist für diese Daten. Sie beruht auf der gleichen Feststellung und dem gleichen Streben nach Wirksamkeit.

Absatz 6 räumt dem Bundesrat die Möglichkeit ein, bestimmte Personen, die der Definition der Anbieterin von Fernmeldediensten entsprechen, aufgrund von bestimmten Merkmalen von bestimmten Pflichten zu befreien, die eine aktive Vorbereitung ihrerseits erfordern (im Gegensatz zur einfachen Pflicht, eine Überwachung zuzulassen oder verfügbare Daten zu liefern); aufgrund dieser Merkmale ist zum Beispiel anzunehmen, dass die betreffenden Personen grundsätzlich nicht im Besitz von Daten sind, die für eine Überwachung des Fernmeldeverkehrs von Interesse sind. Dies ist beispielsweise bei Personen der Fall, die Fernmeldedienste im Bildungsbereich oder für eine sehr beschränkte Zahl von Kundinnen und Kunden anbieten. Faktisch kommt diese Befreiungsmöglichkeit der Situation nahe, die nach der heute geltenden Regelung vorgesehen ist. Denn in den persönlichen Geltungsbereich des geltenden BÜPF fallen nur die konzessions- oder meldepflichtigen Anbieterinnen von Fernmeldediensten, und folglich kommen nur ihnen Pflichten aus dem BÜPF zu (Art. 1 Abs. 2 des geltenden BÜPF in Verbindung mit Art. 4 Abs. 2 FMG und 3 FDV). *Absatz 6* verpflichtet die betreffenden Anbieterinnen, die Randdaten zu liefern, über die sie allenfalls verfügen. Im Gegensatz zur allgemeinen Regel (siehe Abs. 5) besteht für sie jedoch keine Pflicht, diese Daten aufzubewahren. Den erfassten Personen werden jedoch die Minimalpflicht, eine Überwachung zu dulden, sowie die notwendigen Nebenpflichten auferlegt, um die Durchführung einer Überwachung zu ermöglichen (siehe Abs. 2). Allerdings ist zu beachten, dass sich die Lücke, die sich aus *Absatz 6* ergibt, mit diesen Pflichten nicht vollständig schliessen lässt, denn die vorgeschlagene Regelung kann zur Folge haben, dass Randdaten verloren gehen, die normalerweise im Rahmen einer rückwirkenden Überwachung beschafft werden können. Auch Daten, die sich normalerweise im Rahmen einer Echtzeit-Überwachung beschaffen lassen, können verloren gehen; dies, weil sich die Reaktionszeit für die Einleitung der Überwachung verlängert, da der Dienst oder die von ihm beauftragte Person dafür Zeit benötigt.

Im Gegensatz zu dem, was die Motion Glanzmann-Hunkeler 07.3627 (Registrierungspflicht bei Wireless-Prepaid-Karten) verlangt, und obwohl dadurch eine Lücke in der Überwachung zugelassen wird, verpflichtet der vorliegende Entwurf die Anbieterinnen von Fernmeldediensten nicht, die Benutzerinnen und Benutzer (und nicht bloss deren Computer) der von ihnen bereitgestellten Netze zu identifizieren, die eine Person diesen Benutzerinnen und Benutzern zur Verfügung stellt Siehe im Übrigen die Erläuterungen zu Artikel 29.

Art. 27 Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste

Einleitend ist festzuhalten, dass in *Artikel 27* keine allzu hohen Erwartungen gesetzt werden sollten, da viele bedeutende Anbieterinnen der entsprechenden Internetdienste ihren Sitz und ihre Infrastruktur im Ausland haben. Siehe im Übrigen die Erläuterungen zu Artikel 2 Buchstabe c.

Absatz *1* auferlegt den erfassten Anbieterinnen die Minimalpflicht, eine Überwachung zu dulden, sowie die notwendigen Nebenpflichten, um die Durchführung dieser Überwachung zu ermöglichen. Die Überwachung bezieht sich auf Daten, welche die überwachte Person über eine solche Anbieterin versendet (z.B. bei Email-Diensten) oder bei dieser speichert (z.B. bei Cloud Storage-Diensten). Es wird vorgesehen, dass der Dienst oder eine von ihm beauftragte Person, namentlich die Polizei, die Überwachung ausführt. Dies bedeutet nicht, dass der Dienst im Sinne von Artikel 178 Absatz 3 BV Verwaltungsaufgaben an Private übertragen kann. Der Dienst ist weiterhin für die Durchführung der betreffenden Aufgabe verantwortlich.

Absatz 2 verpflichtet die erfassten Personen, die Randdaten zu liefern, über die sie allenfalls verfügen (zumindest jene, über die sie zum Zeitpunkt der Überwachungsverfügung verfügen). Im Gegensatz zur Vorschrift, die grundsätzlich für die Anbieterinnen von Fernmeldediensten gilt (siehe Art. 26 Abs. 5), besteht für die erfasstem Personen jedoch keine Pflicht, diese Daten aufzubewahren. Gegenüber der normalen Regelung, die für die Anbieterinnen von Fernmeldediensten gilt, kann diese Regelung zur Folge haben, dass Randdaten verloren gehen, die im Rahmen einer rückwirkenden Überwachung beschafft werden können. Auch Daten, die sich im Rahmen einer Echtzeit-Überwachung beschaffen lassen, können verloren gehen, dies, weil sich die Reaktionszeit für die Einleitung der Überwachung verlängert, da der Dienst oder die von ihm beauftragte Person dafür Zeit benötigt.

Die Herausgabe von Randdaten ist grundsätzlich eine rückwirkende Überwachung und stellt einen Spezialfall der strafprozessualen Beschlagnahme (Art. 263 ff. StPO) dar, denn anders als bei der Echtzeit-Überwachung werden bereits vorbestehende Daten aus dem Fernmeldeverkehr einer überwachten Person bei einer Anbieterin beschlagnahmt. Eine solche Herausgabe ist deshalb ein Spezialfall, weil diese Daten zum Kommunikationsinhalt gehören: Damit die (in Echtzeit) abgefangene Information sachlich und rechtlich korrekt eingeordnet werden kann, sind weitere Informationen notwendig, beispielsweise Randdaten (wie oft hat eine bestimmte Person eine bestimmte Website angesurft, zu welchen Zeiten etc.). Es ist nicht nur wichtig zu wissen, was eine Person gesagt hat, sondern auch, wann und mit wem sie dies tat. Diese Informationen fallen naturgemäss bei den Anbieterinnen der jeweiligen Dienste an, weshalb diese gemäss BÜPF gegebenenfalls – je nach Anbietertyp, vgl. Artikel 2 – verpflichtet sind, Randdaten zu speichern bzw. soweit vorhanden herauszugeben; es müssen auch weitere Informationen herausgegeben werden, falls sie für die Strafverfolgung notwendig sind.

Diese Herausgabepflicht ist nichts Neues, sondern findet sich bereits in den herkömmlichen strafprozessualen Regeln (Art. 263 ff. StPO). Hinsichtlich des engen Konnexes dieser Daten zum Kommunikationsinhalt und dem Umstand, dass diese Daten bei den Anbieterinnen nach Artikel 2 erhoben werden und diese im Bereich Randdaten teilweise sogar eine Aufbewahrungspflicht trifft, ist diese besondere Art der Beschlagnahme mittels spezialgesetzlicher Grundlage sachlich richtig im BÜPF zu regeln (z.B. Art. 21, 22, 27 Abs. 2, 28 Abs. 2 etc.).

Das vorstehend Ausgeführte trifft generell auf die Herausgabe von Randdaten zu (vgl. Art. 8 Bst. b, Art. 19 Abs. 1 Bst. b und Art. 26 Abs. 1 Bst. b), aber beispielsweise auch auf Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet, welche etwa bei einer Anbieterin von Cloud-Services erhoben werden (vgl. Art. 22). Die Regelung dieser speziellen Editionspflichten im BÜPF hat zudem den rechtsstaatlichen Vorteil, dass die Strafverfolgung höhere Hürden zu überwinden hat, um an die gewünschten Informationen zu gelangen: Für die Anordnung der

Beschlagnahme (d.h. die Überwachungsanordnung) muss die Genehmigung des Zwangsmassnahmengerichts zwingend vorliegen (Art. 269 i.V.m. Art. 272 StPO), was den Rechtsschutz der beschuldigten Person verstärkt. Bei einer klassischen Beschlagnahme nach Artikel 263 StPO ist dies nicht erforderlich, und das (Zwangsmassnahme-) Gericht wird einzig im Rahmen einer Siegelung (bzw. bei einem Entsiegelungsgesuch, vgl. Art. 248 StPO) tätig.[53]

Unter Umständen gelangt der Bundesrat allerdings zum Schluss, dass die in Absatz 1 und 2 vorgesehene Regelung für eine angemessene Überwachung nicht ausreicht. Deshalb ermöglicht ihm *Absatz 3*, den erfassten Personen zusätzliche Pflichten zu übertragen. Als Modell dienen dabei die Pflichten, die von den Fernmeldedienstanbieterinnen erfüllt werden müssen. Der Bundesrat kann somit diesen Personen Pflichten übertragen, die im Gegensatz zur einfachen Pflicht nach Absatz 1 und 2eine aktive Vorbereitung ihrerseits erfordern. In diesem äusserst technischen Bereich, der sich laufend weiterentwickelt, lässt sich keine sinnvolle Delegationsnorm mit einem höheren Bestimmtheitsgrad vorsehen. Diese Vorschrift enthält zudem einschränkende Kriterien, die sich konkreter gestalten lassen. Sie ist somit zulässig. Sie ist vor allem deshalb gerechtfertigt, weil sie einen technischen Bereich betrifft, der sich insbesondere bezüglich der Akteure und der angebotenen Dienste rasant entwickelt. Deshalb muss die anwendbare Gesetzgebung rasch an die neuen Bedürfnisse im Bereich der Überwachung angepasst werden können. Mit dem Begriff der Notwendigkeit, der in dieser Norm enthalten ist, wird Bezug auf Situationen genommen, die wiederholt aufgetreten sind oder die sich in Zukunft immer wieder stellen werden und in denen sich die gewünschten Daten mit den Pflichten nach Absatz 1 und 2 nicht beschaffen lassen (siehe die Erläuterungen zu Abs. 1 und 2). In diesen Situationen ist es somit vernünftig, die betreffenden Anbieterinnen Überwachungspflichten zu unterstellen, die weiter gehen als die einfache Pflicht, die Überwachung zu dulden oder verfügbare Daten zu liefern. Auch in zwei weiteren Kriterien, die in *Absatz 3* genannt werden, kommt zum Ausdruck, dass die Unterstellung dieser Anbieterinnen unter weitergehende Pflichten angemessen sein muss: Die betreffenden Anbieterinnen müssen Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten. Es obliegt dem Bundesrat, diese Kriterien zu konkretisieren und zu bestimmen, ob sie in einem bestimmten Fall erfüllt sind. Gestützt auf diese Delegationsnorm wird der Bundesrat festlegen, dass die bestehenden Überwachungsmöglichkeiten beibehalten werden. Er wird insbesondere festlegen, dass die zusätzlichen Pflichten aus dieser Bestimmung für die E-Mail-Dienste gelten, die von grossen Unternehmen angeboten werden; in der geltenden VÜPF ist dies bereits für die Anbieterinnen von Post- und Fernmeldediensten vorgesehen. Andernfalls werden nach dem neuen BÜPF weniger umfangreiche Überwachungsmöglichkeiten zur Verfügung stehen als nach dem geltenden Gesetz, was mit dem vorrangigen Ziel dieser Totalrevision nicht zu vereinbaren ist.

Nutzt der Bundesrat die Kompetenz, die ihm in *Absatz 3* erteilt wird, sind die in diesem Entwurf vorgesehenen Bestimmungen zu den Überwachungen, die von den Fernmeldedienstanbieterinnen auszuführen sind, sinngemäss anwendbar. Diesfalls unterstellt der Bundesrat die Personen nach Artikel 2 Buchstabe c allen oder einem Teil der Pflichten der Anbieterinnen von Fernmeldediensten. In diesem Fall gelten

53 Vgl. auch Marc Jean-Richard-dit-Bressel in: Niggli/Heer/Wiprächtiger (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011, Art. 269 N 20.

für sie auch die Bestimmungen, in denen nur die Anbieterinnen von Fernmeldediensten ausdrücklich genannt werden (z.B. Art. 4, 17 Bst. a–d, 18, 24–25, 32 etc.).

Art. 28 Pflichten der Betreiberinnen von internen Fernmeldenetzen

Artikel 28 Absatz 1 auferlegt den erfassten Personen die hinreichende Minimalpflicht, eine Überwachung zu dulden, sowie die notwendigen Nebenpflichten, um die Durchführung dieser Überwachung zu ermöglichen. Dies entspricht den Pflichten, die den Betreiberinnen von internen Fernmeldenetzen und Hauszentralen nach dem geltenden BÜPF zukommen. Es wird vorgesehen, dass der Dienst oder eine von ihm beauftragte Person, namentlich die Polizei, die Überwachung ausführt. Das bedeutet nicht, dass der Dienst im Sinne von Artikel 178 Absatz 3 BV Verwaltungsaufgaben an Private übertragen kann. Der Dienst ist weiterhin für die Durchführung der betreffenden Aufgabe verantwortlich.

Zudem wird gemäss *Absatz 2* den erfassten Personen die Pflicht auferlegt, die Randdaten zu liefern, über die sie allenfalls verfügen (zumindest jene, über die sie zum Zeitpunkt der Überwachungsverfügung verfügen), ohne sie jedoch zu verpflichten, diese Daten aufzubewahren. Gegenüber der normalen Regelung, die für die Anbieterinnen von Fernmeldediensten gilt, kann diese Regelung zur Folge haben, dass Randdaten verloren gehen, die im Rahmen einer rückwirkenden Überwachung beschafft werden können. Auch Daten, die sich im Rahmen einer Echtzeit-Überwachung beschaffen lassen, können verloren gehen; dies, weil sich die Reaktionszeit für die Einleitung der Überwachung verlängert, da der Dienst oder die von ihm beauftragte Person dafür Zeit benötigt. Dennoch ist es angebracht, den erfassten Personen keine zusätzlichen Pflichten aufzuerlegen, die eine aktive Vorbereitung voraussetzen, denn damit würden unverhältnismässige Anstrengungen von ihnen gefordert. Allerdings könnte die Motion Glanzmann-Hunkeler 07.3627 (Registrierungspflicht bei Wireless-Prepaid-Karten), die in diesem Punkt nicht klar ist, dies möglicherweise verlangen.

Art. 29 Pflichten der Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen

Artikel 29 Absatz 1 auferlegt den erfassten Personen die hinreichende Minimalpflicht, eine Überwachung zu dulden, sowie die notwendigen Nebenpflichten, um die Durchführung dieser Überwachung zu ermöglichen. In Anlehnung an die geltende Regelung wird vorgesehen, dass der Dienst oder eine von ihm beauftragte Person, namentlich die Polizei, die Überwachung ausführt. Das bedeutet nicht, dass der Dienst im Sinne von Artikel 178 Absatz 3 BV Verwaltungsaufgaben an Private übertragen kann. Der Dienst ist weiterhin für die Durchführung der betreffenden Aufgabe verantwortlich.

Zudem wird gemäss *Absatz 2* den erfassten Personen die Pflicht auferlegt, die Randdaten zu liefern, über die sie allenfalls verfügen (zumindest jene, über die sie zum Zeitpunkt der Überwachungsverfügung verfügen), ohne sie jedoch zu verpflichten, diese Daten aufzubewahren. Gegenüber der normalen Regelung, die für die Anbieterinnen von Fernmeldediensten gilt, kann diese Regelung zur Folge haben, dass Randdaten verloren gehen, die im Rahmen einer rückwirkenden Überwachung beschafft werden können. Auch Daten, die sich im Rahmen einer Echtzeit-Überwachung beschaffen lassen, können verloren gehen; dies, weil sich die Reak-

tionszeit für die Einleitung der Überwachung verlängert, da der Dienst oder die von ihm beauftragte Person dafür Zeit benötigt.

Dennoch ist es angebracht, den erfassten Personen keine zusätzlichen Pflichten aufzuerlegen, die eine aktive Vorbereitung voraussetzen, denn damit würden unverhältnismässige Anstrengungen von ihnen gefordert. Dies gilt für die Pflicht zur Benutzeridentifikation, die anscheinend in der Motion Glanzmann-Hunkeler 07.3627 (Registrierungspflicht bei Wireless-Prepaid-Karten) verlangt wird. Eine solche Pflicht zur Identifikation durch die Personen, die unter diesen Artikel fallen, würde zudem praktische Probleme aufwerfen. Bei den erfassten Personen handelt es sich um Privatpersonen oder um Hotels, Restaurants, Cafés, Spitäler, Schulen, Geschäfte, Gemeinden usw., die ihren Zugang Dritten zur Verfügung stellen. Sie müssten ein Register führen und darin gegen Vorlage eines Ausweispapiers festhalten, wann sie welchen Dritten Zugang zu ihrem Netz gewährt haben. Eine solche Registrierung ist mit relativ hohem Aufwand verbunden, nicht unbedingt zuverlässig und möglicherweise kaum mit der Aktivität der Drittperson vereinbar (die zum Beispiel nur rasch einen Kaffee in einer Gaststätte trinken möchte, die Zugang zu ihrem WLAN-Netz bietet).

Die erwähnte Motion scheint zu verlangen, dass eine Pflicht zur Identifikation der Benutzerinnen und Benutzer (und nicht bloss ihrer Computer) von Netzen vorgesehen wird, die Dritten zur Verfügung gestellt werden.

Falls überhaupt eine solche Pflicht eingeführt werden müsste, sollte sie nicht der Person zukommen, die ihr Netz Dritten zur Verfügung stellt, sondern nur der Fernmeldedienstanbieterin, die das betreffende Netz für diese Person bereitstellt. Die Identifikation der Benutzerinnen und Benutzer dieser Netze und von deren Computern, die in Artikel 22 VE-BÜPF vorgesehen war, wurde im Vernehmlassungsverfahren unterschiedlich aufgenommen. Für die Anbieterinnen von Fernmeldediensten scheint sie jedenfalls technisch möglich zu sein. Gemäss den Verfechtern der Identifikationspflicht ist es für ein Hotel oder ein Geschäft einfach, seinen Kunden über einen Code, ein SMS oder die persönliche E-Mail-Adresse einen Zugang zum Internet anzubieten. Die Mehrheit der grossen Anbieterinnen von Fernmeldediensten bieten diese Möglichkeit in der Schweiz bereits an. Dazu kann im konkreten Fall zum Beispiel vom Benutzer verlangt werden, dass er sich vorgängig (beispielsweise mittels seines Mobiltelefons oder seiner Kreditkarte) bei der Fernmeldedienstanbieterin identifiziert, die das Netz für die Person bereitstellt, die es wiederum Dritten zur Verfügung stellt. Die Verfechter einer solchen Identifikation führen ausserdem an, in einigen Nachbarländern der Schweiz und in Schweden sei ein anonymer Zugang zum Internet nicht möglich. Eine solche Regelung mag unter dem Gesichtspunkt der Kriminalitätsbekämpfung berechtigt sein. Allerdings ist zu berücksichtigen, dass für die Anbieterinnen von Fernmeldediensten zusätzlicher Aufwand entstehen würde; vor allem aber würde diese Regelung sehr weit gehen: Sie würde der Freiheit ein Ende setzen, welche die gegenwärtige Betriebsweise der WLAN-Netze bietet; das Ende dieser Netze würde sie allerdings nicht bedeuten. Die Identifikationspflicht wäre womöglich auch kein Allheilmittel, denn sie liesse sich auch technisch umgehen. Trotz dem Inhalt der Motion Glanzmann-Hunkeler 07.3627 (Registrierungspflicht bei Wireless-Prepaid-Karten) und der Tatsache, dass damit eine Lücke in der Überwachung zugelassen wird, sieht der vorliegende Entwurf deshalb vor, auf diese Identifikationspflicht zu verzichten.

Art. 30 Pflichten der professionellen Wiederverkäufer von Karten und ähnlichen Mitteln

Mit *Artikel 30* soll eine Lücke im geltenden Recht geschlossen werden. Dabei geht es um die Registrierung der Daten zur Identität der Kundinnen und Kunden, die von den dieser Bestimmung unterstellten Personen Mittel kaufen, die ohne Abonnementsverhältnis Zugang zu einem öffentlichen Fernmeldenetz bieten. Bisher sind nur die Anbieterinnen von Fernmeldediensten verpflichtet, diese Daten aufzuzeichnen. Erhalten die dieser Bestimmung unterstellten Wiederverkäufer (zum Beispiel Interdiscount, Media Markt und Mobilezone) von den Fernmeldedienstanbieterinnen (zum Beispiel Swisscom, Orange und Sunrise) derartige Mittel – insbesondere Prepaid-SIM-Karten und Prepaid-Wireless-Karten –, die noch nicht auf den Namen eines Kunden registriert sind, müssen sie diese Daten nicht aufzeichnen. Folglich bleibt der betreffende Kunde anonym, was zu einer ungerechtfertigten Lücke in der Überwachung führt. Neu ist vorgesehen, dass die erfassten Personen die Daten aufzeichnen und anschliessend der Fernmeldedienstanbieterin liefern müssen, zu deren Netz das betreffende Mittel Zugang gibt (zum Beispiel Swisscom, Orange und Sunrise), damit diese ihrerseits die Daten aufzeichnen kann. So kann die Fernmeldedienstanbieterin diese Daten nach Massgabe von Artikel 21 und 23 mittels des Systems zur Vermittlung der Auskunftsgesuche über die Fernmeldedienste (CCIS genannt) liefern, das der Dienst in Zusammenarbeit mit den Anbieterinnen von Fernmeldediensten führt. Siehe auch die Erläuterungen zu Artikel 21 Absatz 2. Die Verletzung der Pflichten, die in *Artikel 30* festgelegt sind, wird nach Artikel 39 Absatz 1 Buchstabe c geahndet. Von den Pflichten nach *Artikel 30* nicht betroffen sind die einfachen Telefonkarten, die anstelle von Bargeld zum Telefonieren in den Telefonkabinen verwendet werden können (z.B. die in den Kiosken verkauften, mit Guthaben geladenen «Taxcards»).

2.7 7. Abschnitt: Sicherstellung der Auskunfts- und Überwachungsbereitschaft der Anbieterinnen von Fernmeldediensten

Wie Artikel 18 sind die Artikel 31–34 insbesondere darauf ausgerichtet, eine ordnungsgemässe Ausführung der angeordneten Überwachungen des Fernmeldeverkehrs sicherzustellen. Vor allem soll überprüft werden können, ob die Anbieterinnen von Fernmeldediensten in der Lage sind, nach dem anwendbaren Recht Auskünfte zu erteilen und die betreffenden Fernmeldedienste zu überwachen. Es geht somit um die Einhaltung («Compliance») der entsprechenden Pflichten. In diesem Zusammenhang kann an sich nicht von einer «Zertifizierungs-»Tätigkeit gesprochen werden, wie dies in den Artikeln 18 und 24 des Vorentwurfs vorgesehen war, dient das eingeführte Verfahren doch nicht dazu, die Einhaltung bestimmter Normen für Produkte oder Dienstleistungen zu überprüfen.

Art. 31 Ausführungsbestimmungen über Auskunfts- und Überwachungstypen

Artikel 31 ist eine Delegationsnorm an den Bundesrat (Abs. 1 und 2) und an das EJPD (Abs. 3), welche Einzelheiten bei der Überwachung des Post- und Fernmeldeverkehrs festlegen können. Dabei stellt sich die Frage, welche Einzelheiten denn geregelt werden sollen.

Die Trennung der verwaltungsrechtlichen (BÜPF) von der strafprozessualen (StPO) Seite entspricht einer Forderung in Ziffer 2 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision). Diese getrennte Betrachtung ist sinnvoll, weil das BÜPF einerseits und die StPO andererseits unterschiedliche Adressaten haben und unterschiedliche Regelungszwecke verfolgen; vereinfacht gesagt: Während in der StPO die beschuldigte Person im Fokus steht, geht es im BÜPF um die Anbieterin im Bereich Post- und Fernmeldeverkehr, die bei der strafprozessualen Überwachung der beschuldigten Person mitwirken muss; das BÜPF schliesst also gewissermassen an die StPO an.

Bei oberflächlicher Betrachtung des *Artikels 31* kann der Eindruck entstehen, dass an sich unzulässige, da nicht von einer genügend bestimmten gesetzlichen Grundlage (vgl. Art. 8 Abs. 2 der Konvention vom 4. November 1950[54] zum Schutze der Menschenrechte und Grundfreiheiten [EMRK]; Art. 13 Abs. 1 und Art. 36 Abs. 1 BV) gedeckte Überwachungstypen angeordnet werden könnten. Dies ist jedoch nicht der Fall, da die Artikel 269–279 StPO (insb. Art. 269–269ter in der geänderten Fassung) die strafprozessuale Zulässigkeit in adäquater Weise regeln. Das BÜPF hat sich aber zu diesen strafprozessualen Aspekten nicht zu äussern, sondern soll einzig und allein die technische Umsetzung der strafprozessual zulässigen Überwachungen so weit wie möglich sicherstellen (Notsuche und Fahndung nach verurteilten Personen vorbehalten). Nur in Bezug auf diese technische und verwaltungsrechtliche Seite ist es nötig, die Überwachungstypen im technischen Sinn im BÜPF bzw. in der VÜPF präzise zu regeln.

Gegenüber den überwachten Personen kann, abhängig vom konkreten Fall, jegliche Überwachung des Post- und Fernmeldeverkehrs zulässig sein. Die rechtsstaatliche Absicherung der Grundrechte wird hier nicht über detaillierte Verordnungsbestimmungen gewährleistet, sondern über das strafprozessuale Verfahren: Die Resultate einer Überwachung (in Echtzeit oder rückwirkend; Kommunikationsinhalte oder Randdaten) dürfen ohne richterliche Genehmigung nicht ausgewertet werden; nicht genehmigte Überwachungen werden sofort gestoppt und die gesammelten Daten vernichtet (Art. 277 StPO).

Folgerichtig muss die gesetzliche Grundlage für die Zulässigkeit von Massnahmen wie der Einsatz von GovWare oder IMSI-Catchern und Überwachungstypen wie Kopfschaltungen und Antennensuchläufen in der StPO zu finden sein, diejenige für die Mitwirkung der Fernmeldedienstanbieterinnen im BÜPF[55].

– Aus Sicht des BÜPF sind der Einsatz von GovWare oder IMSI-Catchern irrelevant, da sie keine Mitwirkung von Fernmeldedienstanbietern erfordern. Strafprozessual muss jedoch eine neue gesetzliche Grundlage geschaffen

54 SR **0.101**
55 Dazu auch BGE **130** II 249, 253 ff. und BVGE 2009/46, E. 3.1.3, 3.2, 3.3.

werden, da sie den Rahmen der bisher geregelten Überwachungstypen sprengen (siehe die Erläuterungen zu Art. 269bis und 269ter StPO).

– Antennensuchläufe[56] sind gemäss Literatur und Rechtsprechung[57] strafprozessual unter bestimmten Voraussetzungen zulässig (Randdatenerhebung im Sinne von Art. 273 StPO, aber die Voraussetzungen von Art. 269 Abs. 1 lit. b und c StPO müssen erfüllt sein); eine besondere gesetzliche Grundlage ist nicht erforderlich. Das Bundesgericht qualifiziert den Antennsuchlauf nicht als schweren Grundrechtseingriff, sofern diese Art der Teilnehmeridentifikation die ultima ratio für die konkreten Ermittlungen darstellt, ein dringender Tatverdacht besteht und ein Verbrechen aufgeklärt werden soll, die Täterschaft genügend individualisierbar ist und keine Kommunikationsinhalte erhoben werden[58]. Es bleibt anzumerken, dass der Antennensuchlauf vom Zwangsmassnahmengericht genehmigt werden muss (Art. 273 Abs. 2 StPO) und die Staatsanwaltschaft hierfür die Anordnung und die Begründung (inklusive der wesentlichen Verfahrensakten) dem Gericht zu unterbreiten hat (Art. 274 Abs. 1 StPO). Aus der Perspektive des BÜPF bietet ein Antennensuchlauf keine Besonderheiten, die eine Anpassung des BÜPF erforderten, da ein solcher Suchlauf lediglich eine Form der Beschaffung von Randdaten darstellt und in der geltenden VÜPF bereits geregelt ist (Art. 16 Bst. e VÜPF).

– Kopfschaltungen (Überwachung eines Telefonanschlusses mit einer ausländischen Rufnummer) sind strafprozessual nicht neu, da hier eine bekannte ausländische Rufnummer daraufhin überwacht wird, ob sie von einem sich in der Schweiz befindlichen Teilnehmer angerufen wird. Der Anknüpfungspunkt für die Überwachung bildet – genau wie bei der Überwachung eines nationalen Anschlusses – eine bestimmte Rufnummer. Es liegt keine Überwachung eines Drittanschlusses vor, welche nur unter den Voraussetzungen von Artikel 270 Buchstabe b StPO zulässig ist[59]. Im BÜPF werden lediglich die technische und organisatorische Machbarkeit und die Kostenfolge der Überwachung geregelt[60].

56 Mittels Antennensuchlauf werden in einem ersten Schritt rückwirkend die nicht personenbezogenen Randdaten der gesamten Mobiltelefon-Kommunikation, die innerhalb einer bestimmten Zeit und in einer bestimmten Zelle einer Antenne geführt wurde, erfasst. In einem zweiten Schritt wird mithilfe von verschiedenen vordefinierten Parametern eine Schnittmenge zwischen den erfassten Verbindungen zweier (oder mehrerer) Antennen gebildet; vgl. dazu das Beispiel bei Thomas Hansjakob, a. a. O. (Fussnote 11), Art. 16 VÜPF N 18 und den Sachverhalt in BGE **137** IV 340, 341 f. Diese Überwachungsmassnahme dient der Individualisierung und Identifizierung der Täterschaft bei bereits objektiv konkretisiertem dringendem Verdacht auf ein Verbrechen.

57 Vgl. BGE **130** II 249 und **137** IV 340, 346 ff. (mit Literaturnachweisen).

58 BGE **137** IV 340, 349 ff.

59 Zur missverständlichen Formulierung von Artikel 270 Buchstabe b StPO («Drittperson» anstelle von «Drittanschluss») Thomas Hansjakob, a.a.O. (Fussnote 11), Vorbemerkungen zum BÜPF N 10.

60 Vgl. BVGE 2009/46, E. 3.2, 7.4 und 8.3. Das BVGer stellt hier keine Verletzung von Art. 13 Abs. 1 BV fest. Diese Feststellung erfolgt etwas unvermittelt, denn in E. 3.2 begründet das BVGer das Nichteintreten auf die Rüge der Fernmeldedienstanbieterin, die überwachte Person werde ohne gesetzliche Grundlage in ihren Rechten verletzt.

– Der Vollständigkeit halber sei erwähnt, dass Internetüberwachungen keine besondere gesetzliche Grundlage erfordern, da sie unbestritten[61] unter die Definition des Fernmeldeverkehrs in Artikel 269 StPO und Artikel 1 BÜPF fallen.

Zusammenfassend kann festgehalten werden, dass die gesetzliche Grundlage für die Frage, *ob* eine Überwachung überhaupt zulässig ist, in Artikel 269 ff. StPO zu finden ist (strafprozessuale Seite). Hingegen ist die Frage, *wie* die im Rahmen des Post- und Fernmeldeverkehrs tätigen Akteure bei einer solchen Überwachung zur Mitwirkung verpflichtet werden können, im BÜPF geregelt (verwaltungsrechtliche Seite). Siehe dazu auch die Erläuterungen zu Artikel 42.

Absätze 1 und 2 stellen eine Delegationsnorm dar, mit der dem Bundesrat die Kompetenz erteilt wird, Fragen zu regeln, die er bereits heute in der VÜPF regelt. Mit dieser Regelung lässt sich zum Beispiel berücksichtigen, dass man im Rahmen einer rückwirkenden Überwachung eines Telefonverkehrs, einschliesslich des Internettelefonverkehrs, von einer Anbieterin von Fernmeldediensten nicht zwangsläufig die gleichen Randdaten anfordern können muss wie bei einer rückwirkenden Internetüberwachung (die sich auf andere Aspekte als den Telefonverkehr bezieht). Bei einer rückwirkenden Internetüberwachung darf es beispielsweise nicht in jedem Fall möglich sein, zu erfahren, welche Internetseiten abgerufen wurden. Denn auch wenn sich ein solcher Überwachungstyp nur auf Randdaten bezieht, läuft er im Grunde faktisch darauf hinaus, dass er eine gewisse Überwachung des Inhalts des Fernmeldeverkehrs ermöglicht. Die vom Bundesrat gestützt auf die *Absätze 1 und 2* vorgeschlagenen Bestimmungen werden den betroffenen Kreisen in einer Vernehmlassung bzw. Anhörung unterbreitet werden. Es ist zu erwähnen, dass zwar auch Überwachungen eines neuen Typs durchgeführt werden können, der in den Ausführungsbestimmungen noch nicht aufgeführt ist, aber dennoch durch die StPO abgedeckt wird. In der Konsequenz obliegt der Fernmeldedienstanbieterin in einem solchen Fall – wie grundsätzlich auch die Anbieterinnen abgeleiteter Kommunikationsdienste (Art. 27) oder den Betreiberinnen von internen Fernmeldenetzen (Art. 28) – jedoch nicht die Pflicht, die Überwachung selber durchzuführen, sondern nur die Pflicht, diese Überwachung durch den Dienst oder durch von diesem beauftragte Dritte zu ermöglichen und zu dulden (vgl. Art. 26 Abs. 2 und 32 Abs. 2).

Absatz 3 sieht vor, dass die technischen und administrativen Einzelheiten, mit denen die ordnungsgemässe, möglichst kostengünstige Ausführung der üblichen zulässigen Überwachungstypen sichergestellt werden soll, nicht mehr wie bisher in Weisungen des Dienstes, sondern in Verordnungsbestimmungen des EJPD geregelt werden. Es ist vorgesehen, die sehr technischen und umfangreichen Verordnungsbestimmungen nur mittels Verweis in der Amtlichen Sammlung des Bundesrechts aufzunehmen (Art. 5 des Bundesgesetzes vom 18. Juni 2004[62] über die Sammlungen des Bundesrechts und das Bundesblatt); diesfalls fände sich der vollständige Text auf der Homepage des EJPD.

Die Regelung der technischen und administrativen Einzelheiten in einer Verordnung bedeutet, dass die Durchführung dieser Überwachungen standardisiert wird. Da in diesem Bereich internationale Standards bestehen, ist es angebracht, diese zu berücksichtigen. Es giltklarzustellen, dass nicht zwangsläufig alle zulässigen Über-

61 Vgl. nur Marc Jean-Richard-dit-Bressel in: Niggli/Heer/Wiprächtiger (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011, Art. 269 N 15 f.
62 SR **170.512**

wachungstypen im Sinne von Absatz 1 standardisiert sind. Bei jenen, die zulässig, aber (noch) nicht standardisiert sind, handelt es sich um spezielle Überwachungsmassnahmen, sogenannte Sonderfälle. Die oben vorgesehene Kompetenzänderung entspricht der Stossrichtung von Ziffer 1 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision). In diesen Vorstössen wird verlangt, dass die normsetzenden und regulativen Aufgaben des Dienstes grundsätzlich von seinen Aufgaben im Zusammenhang mit der Durchführung der Überwachungen zu trennen sind. Aufgrund dieser Änderung werden die betreffenden Bestimmungen auch besser legitimiert sein; sie können namentlich im beratenden Organ nach Artikel 5 dieses Entwurfes erarbeitet werden.

Art. 32 Auskunfts- und Überwachungsbereitschaft

Unter *Artikel 32* fallen selbstverständlich nur jene Überwachungstypen, von deren Ausführung die Fernmeldedienstanbieterin nicht nach Artikel 26 Absatz 6 befreit ist.

Nach *Absatz 1* muss die Erteilung der Auskünfte und die Ausführung der Überwachungen nach dem anwendbaren Recht erfolgen, insbesondere unter Einhaltung der Modalitäten, die im BÜPF, in der VÜPF sowie in den Verordnungen festgelegt sind, in denen die technischen und administrativen Einzelheiten geregelt sind. Die Fernmeldedienstanbieterinnen müssen über die Auskünfte und Daten verfügen müssen, damit sie ihrer Pflicht nach Erteilung der Auskünfte und Lieferung der Daten nachkommen können. Dies bedeutet, dass sie diese Auskünfte und die Randdaten aufbewahren müssen.

Die Pflicht in *Absatz 2* setzt ein aktives Verhalten der Fernmeldedienstanbieterinnen gemäss den Anweisungen des Dienstes voraus (Art. 16 Bst. d). Folglich müssen sie insbesondere die für die Durchführung der Überwachung notwendigen Auskünfte erteilen und bei Bedarf Zutritt zu ihren Anlagen gewähren.

Absatz 3 sieht vor, dass die Anbieterinnen von Fernmeldediensten die Erfüllung der Gesamtheit oder eines Teils der ihnen zukommenden Auskunfts- und Überwachungspflichten auf eigene Kosten Dritten übertragen können. Dabei handelt es sich in erster Linie um Unternehmen, die sich darauf spezialisiert haben, Dienstleistungen im Bereich der Überwachung des Fernmeldeverkehrs auf Anordnung der Behörden anzubieten (*lawful interception*). Die vorgesehene Regelung bietet grosse Flexibilität. In der Praxis bedeutet sie vor allem, dass die Anbieterinnen von Fernmeldediensten nicht gezwungen sind, eine Infrastruktur anzuschaffen, um die festgelegten Pflichten zu erfüllen. Nach der vorgeschlagenen Regelung können sich die Anbieterinnen zum Beispiel auch zusammentun, um diesen Pflichten nachzukommen, wobei es im Übrigen nicht von Belang ist, ob sie die notwendige Infrastruktur kaufen oder mieten. Um den Anforderungen von Absatz 1 gerecht zu werden, genügt es somit nach dem Wortlaut von *Absatz 3*, dass die betreffende Fernmeldedienstanbieterin in der Lage ist, die Erteilung der jeweiligen Auskünfte und die Ausführung der Überwachungen über eine Drittperson oder in Zusammenarbeit mit dieser sicherzustellen. Die Auskunfts- und Überwachungspflichten kommen jedoch weiterhin einzig den Anbieterinnen von Fernmeldediensten zu, nicht den Drittunternehmen, die allenfalls zur Erfüllung dieser Pflichten beigezogen werden. Siehe im Übrigen die Erläuterungen zu Artikel 33 Absatz 1. Der *zweite Satz von Absatz 3* betrifft die privatrechtliche Beziehung zwischen den Anbieterinnen von Fernmeldediensten und den Dritten, die unter Umständen mit der Erfüllung der oben genannten Pflichten betraut werden. Der *dritte Satz von*

Absatz 3, der sich auf die verwaltungsrechtliche Beziehung zwischen dem Dienst und dieser Drittperson bezieht, soll insbesondere den reibungslosen Ablauf der Überwachung gewährleisten, dies auch in Bezug auf den Schutz und die Qualität der Daten.

Art. 33 Nachweis der Auskunfts- und Überwachungsbereitschaft

Gemäss dieser Bestimmung müssen die Anbieterinnen von Fernmeldediensten belegen, dass sie die Erteilung der Auskünfte und die Ausführung der Überwachungen nach dem anwendbaren Recht sicherstellen können. Vor allem müssen sie dabei die Modalitäten einhalten, die im BÜPF, in der VÜPF sowie in den Verordnungen festgelegt sind, in denen die technischen und administrativen Einzelheiten geregelt sind. Die Fernmeldedienstanbieterinnen tragen die Kosten, die mit dem Nachweis nach *Absatz 1* verbunden sind, und somit auch die Kosten, die anfallen, wenn zur Erbringung dieses Nachweises ein Drittunternehmen beigezogen wird. Selbstverständlich müssen die Anbieterinnen von Fernmeldediensten diesen Nachweis nur für jene Überwachungstypen erbringen, von deren Ausführung sie nicht nach Artikel 26 Absatz 6 befreit sind. Diese Pflicht setzt ein aktives Verhalten der Fernmeldedienstanbieterin voraus. Folglich müssen sie insbesondere die für diesen Nachweis notwendigen Auskünfte erteilen und bei Bedarf Zutritt zu ihren Anlagen gewähren. Unter Umständen kann eine Fernmeldedienstanbieterin den ihr zukommenden Auskunfts- und Überwachungspflichten nur über eine Drittperson, die sie mit der Erfüllung der Gesamtheit oder eines Teils dieser Pflichten betraut hat, oder in Zusammenarbeit mit dieser nachkommen. Dies ist gemäss Artikel 32 Absatz 3 zulässig. In diesem Fall kann diese Drittperson aufgefordert werden, dass sie die notwendigen Schritte unternimmt – und die betreffende Fernmeldedienstanbieterin bei der Erfüllung ihrer Nachweispflicht nach *Absatz 1* unterstützt –, um gegenüber dem Dienst zu beweisen, dass sie in der Lage ist, anstelle der Fernmeldedienstanbieterin oder in Zusammenarbeit mit dieser den erwähnten Auskunfts- und Überwachungspflichten nachzukommen. Gelingt es der Drittperson nicht, diesen Nachweis zu erbringen, ist dies der Fernmeldedienstanbieterin zur Last zu legen. Siehe im Übrigen die Erläuterungen zu Artikel 32 Absatz 3.

Da die Überprüfung, ob eine Fernmeldedienstanbieterin den Nachweis für ihre Auskunfts- und Überwachungsbereitschaft erbracht hat, sehr aufwendig sein kann und der Dienst unter Umständen nicht über das erforderliche Personal verfügt, kann er Dritte mit dieser Überprüfung beauftragen. Dies bedeutet nicht, dass er im Sinne von Artikel 178 Absatz 3 BV Verwaltungsaufgaben an Private übertragen kann. Der Dienst ist weiterhin für die Durchführung dieser Aufgabe verantwortlich. Falls er von dieser Möglichkeit Gebrauch macht, kommt ihm jedoch nach Absatz 6 weiterhin die Aufgabe zu, den Anbieterinnen von Fernmeldediensten eine Bestätigung auszustellen, wenn sie den erwähnten Nachweis erbracht haben. Dies setzt voraus, dass der Dienst kontrolliert, ob die von ihm beauftragte Drittperson bei der durchgeführten Überprüfung die festgelegten Modalitäten eingehalten hat.

Basierend auf *Absatz 3* können der Dienst und die Fernmeldedienstanbieterin auch Qualitätskontrollen durchführen, indem zum Beispiel fiktive Testziele überwacht werden (siehe Art. 18 und die entsprechenden Erläuterungen).

Nach *Absatz 4* muss die überprüfte Fernmeldedienstanbieterin dem Dienst eine Gebühr als Entschädigung für die Leistung entrichten, die er erbracht hat. Diese Gebühr wird vom Bundesrat entsprechend der Art der vom Dienst erbrachten Leistung festgesetzt.

Absatz 5 kommt Artikel 16 Buchstabe d nahe. Dieser bezieht sich jedoch nicht auf ein Verfahren zum Nachweis der Auskunfts- und Überwachungsbereitschaft, das auch im Anschluss an eine nicht optimal verlaufene Überwachung erfolgen kann, sondern auf ein Verfahren im Zusammenhang mit der Ausführung einer Überwachung. Die Anbieterinnen von Fernmeldediensten tragen die Kosten der Massnahmen, die sie treffen müssen, um Mängel im Zusammenhang mit der Auskunfts- und Überwachungsbereitschaft zu beheben, da diese Massnahmen notwendig sind, damit die Anbieterinnen ihre gesetzlichen Pflichten erfüllen können. Kommt eine Anbieterin den Anweisungen des Dienstes, technische und organisatorische Massnahmen zu treffen, um Mängel im Zusammenhang mit der Auskunfts- und Überwachungsbereitschaft zu beheben, nicht nach, so kann sie nach Artikel 39 Absatz 1 Buchstabe a bestraft werden.

Der Inhalt der Bestätigung und die Details der Gültigkeitsdauer werden nach *Absatz 6* vom Bundesrat auf dem Verordnungsweg festgelegt. In der Bestätigung muss insbesondere der materielle Geltungsbereich aufgeführt sein, d.h. auf welche Auskünfte und Überwachungstypen sich der betreffende Nachweis bezieht. Ausserdem muss der zeitliche Geltungsbereich angegeben sein, d.h. wie lange die Bestätigung gültig ist, insbesondere im Fall von technischen Weiterentwicklungen. Aufgrund dieser Bestätigung kann davon ausgegangen werden, dass die Anbieterin von Fernmeldediensten in der Lage ist, die Auskünfte zu erteilen und die Überwachungstypen auszuführen, auf die sich die Bestätigung bezieht. Sie ermöglicht es der Fernmeldedienstanbieterin somit, geltend zu machen, dass sie in Bezug auf diese Auskünfte und Überwachungen die Pflicht erfüllt, die ihr nach Absatz 1 zukommt. Für eine Anbieterin von Fernmeldediensten hat diese Bestätigung auch finanzielle Auswirkungen, wenn sich in einem konkreten Fall herausstellt, dass die Anbieterin nicht in der Lage ist, eine Überwachung auszuführen (siehe Art. 34, insbesondere Abs. 2 Bst. a).

Art. 34 Kostenübernahme bei unzureichender Mitwirkung

Artikel 34 ist auf zwei Typen von unzureichender Überwachungsbereitschaft ausgerichtet: Erfasst wird zum einen der Fall, dass eine Anbieterin von Fernmeldediensten zwar willens, aber nicht in der Lage ist, die betreffende Überwachung auszuführen. Zum anderen wird der Fall abgedeckt, dass sich die Anbieterin weigert, der Überwachungsanweisung des Dienstes Folge zu leisten.

Absatz 1 gelangt zur Anwendung, wenn die Anbieterinnen von Fernmeldediensten in einem konkreten Fall nicht in der Lage oder nicht willens sind, die Überwachungen nach dem anwendbaren Recht auszuführen, d.h. insbesondere unter Einhaltung der Modalitäten, die im BÜPF, in der VÜPF sowie in den Verordnungen festgelegt sind, in denen die technischen und administrativen Einzelheiten geregelt sind. Unter diesen Absatz fallen selbstverständlich nur jene Überwachungstypen, von deren Ausführung die Fernmeldedienstanbieterin nicht nach Artikel 26 Absatz 6 befreit ist. Betraut eine Fernmeldedienstanbieterin ein Drittunternehmen mit der Erfüllung der Gesamtheit oder eines Teils der ihr zukommenden Überwachungspflichten, und gelingt es diesem nicht, diese Aufgabe zu wahrzunehmen, ist dies der Fernmeldedienstanbieterin zur Last zu legen. Folglich muss sie auch in diesem Fall die in *Absatz 1* erwähnten Folgen tragen. Siehe im Übrigen die Erläuterungen zu Artikel 31 und 32.

Absatz 2 regelt die Ausnahmen der Kostenübernahme gemäss Absatz 1 und soll für die Anbieterinnen von Fernmeldediensten einen Anreiz darstellen, sich zertifizieren zu lassen. Die Befreiung von der Kostenübernahme kommt selbstverständlich nur zum Tragen, wenn eine Fernmeldedienstanbieterin zwar willens, aber nicht in der Lage ist, die betreffende Überwachung auszuführen. Der Inhalt von *Absatz 2 Buchstabe a* versteht sich von selbst. Eine Fernmeldedienstanbieterin, die über eine Bestätigung nach Artikel 33 Absatz 6 verfügt, muss die jeweiligen Kosten nicht tragen, da aufgrund dieser Bestätigung davon ausgegangen werden kann, dass sie in der Lage ist, die Überwachungstypen auszuführen, auf die sich die Bestätigung bezieht. Ebenso ist es gerechtfertigt, dass die Fernmeldedienstanbieterin im Fall, der in *Absatz 2 Buchstabe b* vorgesehen ist, nicht die finanziellen Auswirkungen tragen muss, die sich aus dem Scheitern der angeordneten Überwachung ergeben. Diese Bestimmung ist insbesondere auf den Fall ausgerichtet, dass der Dienst noch keine Möglichkeit hatte, die betreffende Anbieterin zu überprüfen, vor allem weil ihm die erforderlichen Mittel fehlen.

2.8 8. Abschnitt: Notsuche und Fahndung nach verurteilten Personen

Art. 35 Notsuche

Artikel 35 ist nicht in die StPO aufzunehmen, da sich die Regelung nicht auf ein laufendes Strafverfahren bezieht. Dieser Artikel gilt überdies nicht für den Fall, dass eine Person eine andere entführt oder ihrer Freiheit beraubt, denn ein solcher Fall würde ein Strafverfahren betreffen. Die Mittel zur Überwachung des Post- und Fernmeldeverkehrs zur Lokalisierung des Urhebers dieser Tat können von der Staatsanwaltschaft unmittelbar angeordnet werden. Sofern die entsprechenden Voraussetzungen erfüllt sind, gilt *Artikel 35* hingegen dann, wenn Personen infolge einer Katastrophe (Überschwemmung, Erdbeben usw.) gesucht werden.

Wie Artikel 3 des geltenden BÜPF sieht Artikel 27 VE-BÜPF vor, dass sich die Überwachung des Post- und Fernmeldeverkehrs bei einer Notsuche auf die Teilnehmeridentifikation und die Verkehrsdaten, d.h. auf Randdaten, beschränkt. Nach *Absatz 1* ist dies nicht mehr der Fall. Neu ist es auch möglich, im Bereich des Postverkehrs den Inhalt der Sendungen und im Bereich des Fernmeldeverkehrs jenen der Kommunikation zu erhalten. Dies ist gerechtfertigt, da der Inhalt der Sendungen und der Kommunikation Hinweise auf den Ort liefern kann, an dem sich die vermisste Person befindet, und durch die Überprüfung im Bereich des Fernmeldeverkehrs in Erfahrung gebracht werden kann, ob z.B. der überwachte Anschluss tatsächlich von der vermissten Person benutzt wird. In den Artikeln 19–32 und den in der VÜPF enthaltenen Ausführungsbestimmungen präzsieren, welche Typen der Überwachung des Post- und Fernmeldeverkehrs im Sinne von Artikel 269 StPO angeordnet werden können und wem welche Pflichten bei der Ausführung des jeweiligen Überwachungstyps zukommen.

Die in Artikel 3 Absatz 2 des geltenden BÜPF vorgsehene Bedingung, dass der Aufenthaltsort der vermissten Person nicht bekannt ist, wird in *Absatz 2* durch eine weitere Bedingung ergänzt: den unverhältnismässig schwer zu ermittelnden Aufenthalt. Diese Ergänzung ist gerechtfertigt, denn bei wörtlicher Auslegung stellt die Bedingung des unbekannten Aufenthalts angesichts des Rechtsguts, das auf dem

Spiel steht, übertriebene und unverhältnismässige Anforderungen. Eine Überwachung, wie in den Artikeln 269 Absatz 1 Buchstabe c StPO und Artikel 36 Absatz 1 vorgesehen ist, soll neu möglich sein, wenn die anderen bereits getroffenen Massnahmen zum Auffinden der vermissten Person erfolglos geblieben sind oder wenn die Suche ohne Überwachung aussichtslos wäre oder unverhältnismässig erschwert würde.

Für die Suche nach einer vermissten Person ist gemäss *Absatz 3* auch der Einsatz von technischen Überwachungsgeräten nach Artikel 269bis StPO zulässig. Konkret ermöglicht dies, zu diesem Zweck Geräte wie IMSI-Catcher einzusetzen. Mit dieser leistungsfähigen Überwachungsart lässt sich eine vermisste Person möglicherweise selbst dann auffinden, wenn sich die klassischen Massnahmen der Fernmeldeüberwachung als unwirksam erwiesen haben. Der Einsatz dieser Geräte erfolgt jedoch subsidiär zur Durchführung dieser Überwachungsmassnahmen (siehe sinngemäss die Erläuterungen zu Art. 269bis Bst. b StPO). Dieses Vorgehen (Einsatz von Geräten wie IMSI-Catchern) bedingt nach heutigem Stand keine Intervention einer Fernmeldedienstanbieterin, keinen Verstoss dieser Anbieterin gegen Artikel 321ter Absatz 1 StGB und keinen Einbezug des Dienstes (er muss keine Überwachungsanordnung erhalten). Siehe im Übrigen die Erläuterungen zu Artikel 269bis StPO.

Nach Artikel 3 Absatz 1 des geltenden BÜPF kann in Übereinstimmung mit dem Verfassungsgrundsatz der Verhältnismässigkeit nicht nur der Post- und Fernmeldeverkehr der gesuchten Person, sondern sofern notwendig auch jener einer unbeteiligten Drittperson überwacht werden. Dies ist gemäss *Absatz 4* weiterhin möglich. Eine solche Überwachung ist insbesondere dann angezeigt, wenn davon ausgegangen werden kann, dass die vermisste Person den Anschluss dieser Drittperson benutzt oder auf diesen anruft. Diese Möglichkeit bedeutet eine Einschränkung Dritter in ihrem Recht auf Privatsphäre, welches von der Bundesverfassung und vom Völkerrecht garantiert wird (siehe unten Ziff. 5); diesem Umstand gilt es bei der Genehmigung im Einzelfall Rechnung zu tragen.

Art. 36 Fahndung nach verurteilten Personen

Artikel 36 sieht neu die Möglichkeit vor, durch Überwachung des Post- und Fernmeldeverkehrs nach einer Person zu suchen, gegen die in einem rechtskräftigen und vollstreckbaren Entscheid eine Freiheitsstrafe oder eine freiheitsentziehende Massnahme verhängt wurde. Eine solche Überwachung ist im Rahmen eines laufenden Strafverfahrens möglich. Umso mehr muss sie im Hinblick auf das oben genannte Ziel zulässig sein, denn in diesem Fall besteht nicht mehr bloss ein dringender Verdacht (Art. 269 Abs. 1 Bst. a StPO), sondern es liegt gemäss *Absatz 1* ein rechtskräftiges, vollstreckbares Urteil vor. Diese Möglichkeit drängt sich auch deshalb auf, weil sie im Bereich der internationalen Rechtshilfe in Strafsachen[63] gemäss Artikel 18*a* Absatz 1 IRSG bereits vorgesehen ist.

Es wird darauf verzichtet, in *Absatz 1* eine Mindestdauer in Bezug auf die verhängte Freiheitsstrafe anzugeben, ab der eine Überwachung angeordnet werden kann. Bei ihrem Entscheid über die Anordnung einer Überwachung muss sich die zuständige Behörde vom Grundsatz der Verhältnismässigkeit leiten lassen. In diesem Zusammenhang sind vor allem die folgenden Elemente zu berücksichtigen: die Dauer der verhängten unbedingten Freiheitsstrafe, die Straftat, die zu dieser Strafe geführt hat,

63 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 1 BÜPF N 8.

die allfällige Gefährlichkeit der verurteilten Person und die Kosten der in Betracht gezogenen Überwachung.

Wie die Regelung in Artikel 35 ist auch diese nicht in die StPO aufzunehmen, da vorliegend das Strafverfahren in diesem Stadium bereits abgeschlossen ist. Für Überwachungen, die im Rahmen von Strafverfahren angeordnet werden, gilt grundsätzlich die Bedingung in Artikel 269 Absatz 2 StPO (Deliktskatalog). Diese Bedingung ist nicht auf Überwachungen anwendbar, die darauf ausgerichtet sind, eine Person aufzufinden, die zu einer Freiheitsstrafe verurteilt wurde oder gegen die eine freiheitsentziehende Massnahme angeordnet wurde (siehe den Verweis in Art. 37 Abs. 1). Dies ist namentlich deshalb gerechtfertigt, weil in diesem Fall nicht mehr bloss ein dringender Verdacht besteht (Art. 269 Abs. 1 Bst. a StPO), sondern ein rechtskräftiges, vollstreckbares Urteil vorliegt. Entsprechend den Bestimmungen in den Artikeln 269 Absatz 1 Buchstabe c StPO und Artikel 35 Absatz 2 Buchstabe a E-BÜPF wird diese Überwachungsmassnahme subsidiär zu den anderen Massnahmen angeordnet, die ergriffen werden können, um die gesuchte Person zu finden. Bei der Überwachung des Post- und Fernmeldeverkehrs nach Artikel 36 können nicht nur die Daten, die eine Teilnehmeridentifikation ermöglichen, sowie die Verkehrsdaten, d.h. Randdaten, beschafft werden. Es ist auch möglich, im Bereich des Postverkehrs den Inhalt der Sendungen und im Bereich des Fernmeldeverkehrs jenen der Kommunikation zu erhalten. Dies ist gerechtfertigt, da insbesondere der Inhalt der Sendungen und der Kommunikation Hinweise auf den Ort liefern kann, an dem sich die vermisste Person befindet; ferner kann durch die Überprüfung im Bereich des Fernmeldeverkehrs in Erfahrung gebracht werden, ob z.B. der überwachte Anschluss tatsächlich von der gesuchten Person benutzt wird. In den Artikeln 19–32 und den in der VÜPF enthaltenen Ausführungsbestimmungen ist genauer festgelegt, welche Typen der Überwachung des Post- und Fernmeldeverkehrs im Sinne von Artikel 269 StPO angeordnet werden können und wem welche Pflichten bei der Ausführung des jeweiligen Überwachungstyps zukommen.

Für die Fahndung nach einer verurteilten Person ist gemäss *Absatz 2* auch der Einsatz von technischen Überwachungsgeräten nach Artikel 269bis StPO zulässig. Konkret ermöglicht dies, zu diesem Zweck Geräte wie IMSI-Catcher einzusetzen. Mit dieser leistungsfähigen Überwachungsart lässt sich eine gesuchte Person möglicherweise selbst dann auffinden, wenn sich die klassischen Massnahmen der Fernmeldeüberwachung als unwirksam erwiesen haben. Der Einsatz dieser Geräte erfolgt jedoch subsidiär zur Durchführung dieser Überwachungsmassnahmen (siehe sinngemäss die Erläuterungen zu Art. 269bis Bst. b StPO). Dieses Vorgehen (Einsatz von Geräten wie IMSI-Catchern) bedingt nach heutigem Stand keine Intervention einer Fernmeldedienstanbieterin, keinen Verstoss dieser Anbieterin gegen Artikel 321ter Absatz 1 StGB und keinen Einbezug des Dienstes (er muss keine Überwachungsanordnung erhalten). Siehe im Übrigen die Erläuterungen zu Artikel 269bis StPO.

Gemäss *Absatz 3* kann nicht nur der Post- und Fernmeldeverkehr der gesuchten Person, sondern auch jener einer unbeteiligten Drittperson überwacht werden, sofern die Voraussetzungen von Artikel 270 StPO sinngemäss erfüllt sind. Eine solche Überwachung erfolgt zum Beispiel, wenn davon ausgegangen werden kann, dass die gesuchte Person den Anschluss dieser Drittperson benutzt oder auf diesen anruft. Siehe im Übrigen die Erläuterungen zu Artikel 35 Absatz 4.

Art. 37 Verfahren

Artikel 37 regelt das Verfahren in den Fällen der Artikel 35 und 36.

Im Gegensatz zur Fassung, die im VE-BÜPF vorgesehen war, wird in *Absatz 1*, der sowohl auf Artikel 35 als auch auf Artikel 36 anwendbar ist, der Inhalt von Artikel 3 Absatz 3 des geltenden BÜPF übernommen, der sich jedoch nur auf die Suche nach vermissten Personen bezieht. Für die Überwachung nach Artikel 36 wird insbesondere nicht auf die Liste in Artikel 269 Absatz 2 StPO verwiesen (siehe die Erläuterungen zu Art. 36). Die zitierten Artikel gelten nur sinngemäss, da die StPO laufende Strafverfahren regelt, während die Überwachungen nach den Artikeln 35 f. ausserhalb von Strafverfahren erfolgen.

Absatz 2 sieht vor, dass die im Rahmen einer Notsuche überwachten Personen abweichend von Artikel 279 StPO sobald als möglich über die Überwachung informiert werden. Bei der Fahndung kann es ein Interesse geben, die Überwachung länger geheim zu halten bzw. die Information ganz zu unterlassen z.B. bei nachfolgenden Ermittlungen gegen Fluchthelfer (sinngemäss wie Art. 279 Abs. 2 StPO). Ein solches Interesse ist bei der Notsuche nicht ersichtlich, weshalb für solche Fälle eine abweichende Regelung geboten ist.

Absatz 3 lehnt sich an den Inhalt von Artikel 3 Absatz 4 des geltenden BÜPF an. Er regelt die Zuständigkeit zur Anordnung und Genehmigung einer Überwachung, die Gegenstand der Artikel 35 und 36 bildet, wobei es sich versteht, dass sowohl der Bund als auch die Kantone dafür zuständig sein können. Im Bereich der internationalen Rechtshilfe in Strafsachen sind diese Fragen in Artikel 18*a* IRSG geregelt. Nach Artikel 18*a* Absatz 1 des erwähnten Gesetzes kommt in diesem Bereich die Kompetenz zur Anordnung einer Überwachung, mit welcher der Aufenthalt einer vermissten Person ermittelt werden soll, dem Bundesamt für Justiz zu. Die Tatsache, dass die Überwachung einer Genehmigung bedarf, genauer durch eine richterliche Behörde, hat keinen Zeitverlust bei der Umsetzung der Überwachung zur Folge. Entsprechende Befürchtungen, die im Vernehmlassungsverfahren geäussert wurden, sind somit unbegründet. Denn wie bei einer Überwachung im Rahmen eines Strafverfahrens und gemäss der Auslegung, die für Artikel 274 Absätze 1–3 StPO vorzunehmen ist, kann die angeordnete Überwachung schon anlaufen, bevor sie vom Zwangsmassnahmengericht genehmigt wurde.

2.9 9. Abschnitt: Kosten und Gebühren

Art. 38

Nach geltendem Recht gehen die für eine Überwachung notwendigen Einrichtungen zulasten der Anbieterinnen von Post- und Fernmeldediensten. Diese erhalten aber eine angemessene Entschädigung für die Kosten, die bei der Durchführung einer konkreten Überwachung entstehen. Neben dieser Entschädigung haben die anordnenden Behörden eine Gebühr für die Leistungen des Dienstes zu entrichten (Art. 16 des geltenden BÜPF). Artikel 2 der Verordnung vom 7. April 2004[64] über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF) setzt für jeden Überwachungstyp eine Gesamtgebühr und den

64 SR **780.115.1**

darin enthaltenen Anteil der Entschädigung fest und sieht vor, dass die Gesamtgebühr abweichend vom Wortlaut von Artikel 16 Absatz 1 BÜPF dem Dienst zu entrichten ist; dieser leitet die Entschädigung an die Anbieterinnen weiter. Der Vernehmlassungsentwurf (Art. 30 VE-BÜPF) sah im Zusammenhang mit dem Konsolidierungsprogramm 2011–2013 vor, die Entschädigungen zugunsten der Anbieterinnen ersatzlos aufzuheben.

Die Erhebung und Analyse der Kosten der Post- und Fernmeldeüberwachung waren Gegenstand eines vom Dienst in Auftrag gegebenen externen Berichts vom 12. Juni 2012[65]. Der Bericht sollte dazu beitragen, zu entscheiden, welche Regelung im vorliegenden Entwurf in Bezug auf folgende Punkte zu übernehmen ist: die Finanzierung der Infrastruktur für die Durchführung der Überwachungen, die eventuelle Entschädigung der Anbieterinnen sowie die eventuelle Entrichtung einer Gebühr an den Dienst.

Der Inhalt des Berichts und die verschiedenen Varianten wurden in der Folge sorgfältig untersucht, auch im Hinblick auf die Reduktion der Gebühr, welche das Postulat Recordon 11.4210 (Kosten für die Überwachung des Fernmeldeverkehrs im Rahmen eines Strafverfahrens) verlangt. Geprüft wurde die Variante, gemäss welcher die Anbieterinnen sowohl für die Kosten der Einrichtungen als auch für die Kosten, die bei der Durchführung einer einzelnen Überwachung entstehen, angemessen entschädigt werden. Mit dieser Variante kann insbesondere der Situation der kleinen Fernmeldedienstanbieterinnen besser Rechnung getragen werden, die zwar die Investitionskosten dafür tragen müssten, dass sie Überwachungen durchführen könnten, im Gegenzug aber praktisch nie Überwachungsanordnungen erhalten würden. Dabei ist zu präzisieren, dass diese Anbieterinnen von den grundsätzlichen Verpflichtungen der Fernmeldedienstanbieterinnen befreit werden können (siehe Erläuterungen zu Art. 26 Abs. 6), was auch zu tieferen Investitionskosten führen würde. Auf der Grundlage dieser umfassenden Analyse wurde demnach entgegen dem in die Vernehmlassung geschickten und umstrittenen Vorschlag entschieden, das aktuelle System beizubehalten: Die Anbieterinnen müssen die Einrichtungen für die Umsetzung der Überwachungen weiterhin finanzieren, sie erhalten weiterhin eine angemessene Entschädigung für die Durchführung von Überwachungsmassnahmen, die anordnende Behörde entrichtet dem Dienst für dessen Dienstleistungen in Verbindung mit der Durchführung der Überwachung weiterhin eine Gebühr, und der Bundesrat legt die Höhe der Entschädigungen und Gebühren für die verschiedenen Überwachungsarten fest. Es ist nicht angebracht, die Überwachungspflicht mit der Herausgabepflicht nach Artikel 265 StPO zu vergleichen und mittels eines Analogieschlusses die angemessene Entschädigung der Anbieterinnen für die Durchführung einer Überwachungsanordnung zu verneinen. Falls eine Person ihrer strafprozessualen Herausgabepflicht nicht nachkommt, kann das Beweismittel nämlich beschlagnahmt werden; dies ist bei den Daten, welche mit einer Fernmeldeüberwachung erst noch erhoben werden sollen, gerade nicht der Fall.

Absatz 1 übernimmt und ergänzt Artikel 16 Absatz 1 erster Satz des geltenden BÜPF und stellt klar, dass die *Kosten* für die Einrichtungen zu Lasten der Mitwirkungspflichtigen gehen. Dies umfasst auch die Kosten für die Übermittlung der Daten, welche die Mitwirkungspflichtigen (dem Dienst) liefern müssen. Die Datenlieferung stellt einen Teil der Überwachungsbereitschaft dar und ist dementsprechend von den

65 www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ber-isc-ejpd-fda-pda-d.pdf

Mitwirkungspflichtigen als Bringschuld zu tragen. Diese Bestimmung bedeutet vor allem, dass der Erwerb und der Unterhalt der für eine Überwachung notwendigen Einrichtungen ganz von den Anbieterinnen von Post- und Fernmeldediensten finanziert werden müssen, einschliesslich der Personalkosten für Beschaffung und Unterhalt und die Amortisationskosten. Die Pflichten, welche diese Personen zur Umsetzung der Überwachung und zur hinlänglichen Lieferung der Daten erfüllen müssen, werden im anwendbaren Recht, insbesondere im BÜPF, in der VÜPF und den Verordnungen mit den technischen und administrativen Einzelheiten, geregelt. Diese Pflichten können je nach Person variieren (siehe insbesondere Art. 26 und 27).

Absatz 2 übernimmt im Wesentlichen Artikel 16 Absatz 1 zweiter Satz des geltenden BÜPF und eliminiert einen Redaktionsfehler im deutschen Text (das Element «für Aufwendungen» ist redundant und wird gestrichen). Dieser Absatz betrifft die Kosten, die den Mitwirkungspflichtigen im Zusammenhang mit der Durchführung einer einzelnen Überwachung entstehen, also mit Ausnahme der Kosten für die Einrichtungen, die Gegenstand von Absatz 1 sind. Die Kosten der einzelnen Überwachung werden in den meisten Fällen mehrheitlich aus Personalkosten bestehen, es sind aber auch Sachkosten denkbar. Die Anbieterinnen erhalten für diese Kosten eine angemessene Pauschalentschädigung (beispielsweise 80 % ihrer effektiven, entschädigungsfähigen Kosten, vgl. dazu den geltenden Art. 4*a* Abs. 4 GebV-ÜPF). Es kann also vorkommen, dass die Entschädigung – die vom Bundesrat auf Verordnungsstufe geregelt wird (siehe Abs. 4) – nicht sämtliche effektiven variablen Kosten einer Anbieterin deckt. Dabei darf nicht vergessen werden, dass die Verwendung von Telekommunikationsdiensten für strafbare Handlungen für die Anbieterinnen eine Art Geschäftsrisiko darstellt und dass es die Pflicht einer jeder Bürgerin und eines jeden Bürgers ist, zur Aufklärung von Straftaten beizutragen (gemäss Art. 167 StPO erhalten auch Zeuginnen und Zeugen eine angemessene Entschädigung). Zu präzisieren ist hier, dass zwar der Dienst den Anbieterinnen diese Entschädigung überweist, diese im Grunde genommen aber von der anordnenden Behörde geschuldet ist (für weitere Einzelheiten, siehe die Erläuterungen zu Abs. 3). Absatz 2 verfolgt die Stossrichtung von Ziffer 4 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision).

In *Absatz 3* wird aus Gründen der Klarheit ausdrücklich festgehalten, was sich bereits aus Artikel 16 Absatz 2 des geltenden BÜPF ableiten lässt, also dass die anordnende Behörde dem Dienst eine – vom Bundesrat auf Verordnungsstufe festgesetzte (siehe Abs. 4) – Gebühr für die von ihm erbrachten Leistungen im Zusammenhang mit der Überwachung des Post- und Fernmeldeverkehrs entrichten muss. Dabei wird klargestellt, dass der Dienst von den anordnenden Behörden eine Gesamtgebühr erhebt, die sowohl die Gebühr für die Leistungen des Dienstes (*Bst. a*) als auch die Entschädigung zuhanden der Mitwirkungspflichtigen (*Bst. b*) umfasst; der Dienst leitet die Entschädigung an die Mitwirkungspflichtigen weiter (siehe Abs. 2).

Absatz 4 übernimmt Artikel 16 Absatz 2 des geltenden BÜPF, also die Delegationsnorm, aufgrund welcher der Bundesrat die geltende GebV-ÜPF erlassen konnte. Der Bundesrat ist bei der Überwälzung der aus den Überwachungsmassnahmen entstehenden Kosten an das Kostendeckungs- und Äquivalenzprinzip gebunden. Aufgrund der Tatsache, dass der Dienst seine Aufgaben zurzeit nicht kostendeckend erbringt (Kostendeckungsgrad 54 Prozent im Jahr 2012), stellt sich die Frage, ob es sachgerecht ist, am heutigen (tiefen) Kostendeckungsgrad festzuhalten, ist die Strafverfol-

gung doch eine kantonale Aufgabe. Der Bundesrat wird sich mit dieser Frage bei der Festlegung der durch die anordnenden Behörden zu entrichtenden Gebühren eingehend auseinandersetzen.

An dieser Stelle ist noch anzumerken, dass der Betrag, den die anordnende Behörde dem Dienst als Gebühr bezahlt, als Verfahrenskosten bzw. als Auslagen ganz oder teilweise Dritten, insbesondere der beschuldigten oder verurteilten Person, auferlegt werden kann (Art. 422, 425 und 426 StPO), dies unter Einhaltung der Verfahrensregeln.

2.10 10. Abschnitt: Strafbestimmungen

Art. 39 Übertretungen

Artikel 39 wurde gegenüber der Vernehmlassungsversion geändert, insbesondere unter Berücksichtigung der Änderungen, die in Artikel 40 vorgenommen wurden. Die Artikel 6 und 7 VStrR sind bei der Ermittlung der Täterschaft nach *Artikel 39* anwendbar (siehe Art. 40 und die entsprechenden Erläuterungen).

Mit *Absatz 1* werden im neuen BÜPF Strafbestimmungen eingeführt, die eine wirksame Bestrafung der diesem Gesetz unterstellten Personen ermöglichen sollen, falls diese bestimmten der darin festgelegten Pflichten nicht nachkommen und damit durch ihr Verhalten die angeordneten Überwachungen behindern könnten. Die Erfahrung hat gezeigt, dass die grossen Anbieterinnen von Fernmeldediensten, die zurzeit im Schweizer Markt tätig sind, sich ihrer Pflichten grundsätzlich bewusst sind. Die Höchstbusse, die in *Absatz 1* für die vorsätzliche Begehung der in den Buchstaben a–d aufgeführten strafbaren Handlungen vorgesehen ist, liegt über dem Höchstbetrag von 10 000 Franken der in Artikel 292 StGB (Ungehorsam gegen amtliche Verfügungen) vorgesehenen Busse (vgl. auch Art. 106 Abs. 1 StGB). Vor allem angesichts der Einsparungen, die bei Nichtbeachtung der Vorschriften erzielt werden können, kann der letztere Betrag zu tief sein, um von der Begehung der oben erwähnten strafbaren Handlungen abzuhalten. Selbstverständlich muss die Behörde, welche die Höhe der Busse nach Absatz 1 im Einzelfall festlegt, nach den allgemeinen Grundsätzen die Umstände des Einzelfalles berücksichtigen, wie beispielsweise die Schwere der strafbaren Handlung oder die wirtschaftliche Leistungsfähigkeit des fehlbaren Unternehmens (vgl. Art. 8 VStrR und Art. 106 Abs. 3 StGB). In anderen nebenstrafrechtlichen Übertretungen sind im Übrigen Höchststrafen vorgesehen, die viel höher bzw. tiefer als die 100 000 Franken nach *Absatz 1* sind. Die Bestrafung nach Artikel 39 soll nur subsidiär zu strengeren Strafbestimmungen erfolgen, die gleichzeitig nach anderen Gesetzen erfüllt sein könnten; hierbei ist insbesondere an Begünstigung und an die Verletzung von Geheimnispflichten zu denken, welche auch im StGB eingehend geregelt sind. So sind Konstellationen vorstellbar, in denen eine Handlung sowohl den Tatbestand von Artikel 39 Absatz 1 Buchstabe d erfüllt als auch den schwereren von Artikel 320 oder 321ter StGB. In solchen Fällen soll der Täter nicht nach der milderen Strafbestimmung von *Artikel 39* bestraft werden, da hierzu kein sachlicher Grund besteht.

Absatz 1 Buchstabe a sieht bei Nichtbeachtung der Anweisungen des Dienstes eine analoge Strafe vor wie Artikel 292 StGB. Allerdings dürfte die Sanktion in diesem Artikel nicht abschreckend wirken, kann doch eine dem BÜPF unterstellte Person erhebliche Einsparungen erzielen, wenn sie einer Überwachungsanweisung des

Dienstes nicht nachkommt; diese Anordnung kann auf einer Überwachungsanordnung der zuständigen Behörde, in der Regel der Staatsanwaltschaft, beruhen. Einsparung kann eine dem BÜPF unterstellte Person auch, wenn sie der Anweisung des Dienstes, technische und organisatorische Massnahmen zu treffen, um Mängel im Zusammenhang mit der Auskunfts- und Überwachungsbereitschaft zu beheben (Art. 33 Abs. 5), nicht Folge leistet. Deshalb ist es gerechtfertigt, eine spezifische Bestimmung festzulegen, die eine schwerere Strafe als Artikel 292 StGB vorsieht. Dieser Mechanismus soll auch einen Anreiz für die dem BÜPF unterstellten Personen darstellen, die Anweisungen des Dienstes möglichst rasch zu befolgen. Dennoch können diese Personen die Anweisungen gemäss den Verfahrensbestimmungen des Bundesrechts anfechten (siehe Art. 42). Für die Überprüfung der Gültigkeit der Anweisung des Dienstes durch das ordentliche Strafgericht, das im Anschluss an den Dienst für ein Verfahren nach Artikel 39 Absatz 1 Buchstabe a zuständig ist, gelten die gleichen Regeln wie jene, die von Lehre[66] und Rechtsprechung für den Fall der Verletzung von Artikel 292 StGB entwickelt wurden.

Insbesondere aufgrund der Forderungen in Ziffer 2 der Motion Schweiger 06.3170 (Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf elektronischen Netzwerken) sieht *Absatz 1 Buchstabe b* eine Strafbestimmung vor, die ebenfalls auf eine wirksame Ausführung der angeordneten Überwachungen abzielt. Diese Bestimmung bedroht die Verletzung der Aufbewahrungspflicht für die Randdaten im Bereich des Fernmeldeverkehrs (Art. 26 Abs. 5) mit Strafe. Die in Artikel 292 StGB vorgesehene Strafe ist auch zur Ahndung dieses Verhaltens nicht schwer genug. Ausserdem ist die Bestrafung eines derartigen Verhaltens mit diesem Artikel nicht möglich. Denn er gelangt dann zur Anwendung, wenn eine Behörde die Lieferung bestehender Daten anordnet und diese nicht geliefert werden, nicht jedoch, wenn Daten bereits vor der Aufforderung der Behörde vernichtet wurden oder wenn gar keine Daten gesammelt oder gespeichert wurden. Aus Kohärenzgründen muss die beantragte Strafbestimmung auch für die Verletzung der Aufbewahrungspflicht für die Randdaten im Bereich des Postverkehrs gelten (Art. 19 Abs. 4).

Im Anschluss an das Vernehmlassungsverfahren wurden die in Absatz 1 aufgeführten Straftatbestände durch *Absatz 1 Buchstabe c* ergänzt; die Erfahrung hat gezeigt, dass die für diesen Fall vorgesehene Sanktion notwendig ist, um die betreffenden Pflichten durchzusetzen[67].

Absatz 1 Buchstabe d entspricht im Wesentlichen den Artikeln 12 Absatz 3 und 15 Absatz 7 des geltenden BÜPF. Diese Bestimmung bezieht sich auf alle Fakten, die eine Überwachung des Post- oder Fernmeldeverkehrs betreffen. Dies sind insbesondere die Tatsache der Überwachung an sich sowie alle sie betreffenden Informationen – einschliesslich der einfachen Gesuche nach Artikel 15 –, die gestützt auf das BÜPF zwischen den betroffenen Personen, dem Dienst und den Behörden ausgetauscht werden[68]. Der Begriff «Dritte» in *Buchstabe d* umfasst nicht einen beauftragten Subunternehmer einer mitwirkungspflichtigen Person, welcher über die notwendigen Informationen verfügen müssen, um eine bestimmte Überwachung durchführen zu können. Im Gegensatz zu den Artikeln 12 Absatz 3 und 15 Absatz 7 des geltenden BÜPF unterliegen diese Tatsachen gemäss *Buchstabe d* nicht dem Post- und Fernmeldegeheimnis im Sinne von Artikel 321ter StGB. *Buchstabe d* ist

66 Bernard Corboz, a.a.O., Art. 292 StGB N 11–16.
67 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 19*a* VÜPF N 2.
68 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 15 BÜPF N 26.

nicht auf den Fall anwendbar, dass Inhalts- oder Randdaten, die im Rahmen einer Überwachung des Post- oder Fernmeldeverkehrs gesammelt wurden, gegenüber Dritten offengelegt werden. Dieses Verhalten wird bereits durch Artikel 321ter StGB erfasst und bestraft. Um Irrtümer auszuschliessen, kann es für den Dienst angezeigt sein, die dem persönlichen Geltungsbereich des Gesetzes unterstellten Personen auf die strafrechtlichen Konsequenzen hinzuweisen, welche die Verbreitung der betreffenden Tatsachen und Informationen haben kann.

Nach Artikel 105 Absatz 2 StGB, der aufgrund von Artikel 40 Absatz 1 und von Artikel 2 VStrR anwendbar ist, wird der Versuch nur in den vom Gesetz ausdrücklich vorgesehenen Fällen bestraft. *Absatz 2* enthält eine solche Bestimmung. Hinsichtlich der Konsequenzen, die ein solches Verhalten haben kann und hinsichtlich des Umstandes, dass im Nebenstrafrecht des Bundes für zahlreiche Übertretungen die Versuchsstrafbarkeit vorgesehen ist, sind Versuchshandlungen hinsichtlich der in Buchstabe a–d genannten Übertretungstatbestände als strafwürdig einzustufen.

Absatz 3 regelt die fahrlässige Begehung der genannten Verhaltensweisen. Hinsichtlich der Strafwürdigkeit der fahrlässigen Begehung gilt das soeben Ausgeführte sinngemäss. Die Höchstbusse, die in *Absatz 3* für die fahrlässige Begehung der strafbaren Handlungen vorgesehen ist, liegt ebenfalls über dem Höchstbetrag der in Artikel 106 Absatz 1 StGB vorgesehenen Busse. Angesichts der äusserst negativen Konsequenzen, welche die strafbaren Handlungen für eine wichtige laufende Untersuchung haben können, ist der letztere Betrag in gewissen Fällen ebenfalls zu tief. Siehe im Übrigen die sinngemäss geltenden Erläuterungen zu Absatz 1.

Art. 40 Gerichtsbarkeit

Der in die Vernehmlassung gegebene Vorentwurf (Art. 32 VE-BÜPF) sah vor, dass die Verfolgung und Beurteilung der Straftaten nach Artikel 39 den Kantonen obliege, wie dies grundsätzlich die Regel ist, nicht einer Verwaltungsbehörde des Bundes, im vorliegenden Fall dem Dienst. Dies schloss die Anwendung des VStrR aus. Im Vernehmlassungsverfahren wurde dieser Punkt zu Recht kritisiert. Der vorliegende Entwurf sieht deshalb die gegenteilige Lösung vor, was auch im Nebenstrafrecht üblich ist.

Aus *Absatz 1* ergibt sich, dass die Gehilfenschaft strafbar ist. Angesichts des Inhalts von Artikel 5 VStrR, der aufgrund von Artikel 40 und der Artikel 1 und 2 VStrR anwendbar ist, muss dies nicht ausdrücklich erwähnt werden. Auch die Artikel 6 und 7 VStrR (Widerhandlungen in Geschäftsbetrieben, durch Beauftragte u. dgl.) sind anwendbar, ohne dass dies ausdrücklich erwähnt wird, ebenfalls aufgrund von Artikel 40 und der Artikel 1 und 2 VStrR. Die Regelung in den Artikeln 6 und 7 VStrR ersetzt Absatz 4 von Artikel 31 des Vernehmlassungsentwurfs. Diese Regelung ist sinnvoll, da festzuhalten ist, dass es sich bei den «Personen», die unter die betreffende Strafbestimmung fallen, vor allem um die Anbieterinnen von Post- und Fernmeldediensten, deren Angestellte, deren Führungskräfte und die Unternehmen selbst handelt. Die Verfolgungs- und die Vollstreckungsverjährung für die in Artikel 39 vorgesehenen strafbaren Handlungen unterstehen Artikel 11 VStrR, der durch Artikel 333 Absatz 6 Buchstabe b und e StGB ergänzt wird, bis die entsprechenden Fristen an die neuen Verjährungsfristen des allgemeinen Teils des StGB angepasst werden. Nach diesen Artikeln verjährt die Strafverfolgung für diese strafbaren Handlungen in vier Jahren und die Strafe in 7½ Jahren.

Mit *Absatz 2* wird die Kompetenz zur Verfolgung und Beurteilung der Straftaten nach Artikel 39 dem Dienst übertragen, der sich entsprechend organisieren muss. Dies ist rationeller, als die Kantone damit zu betrauen, wie dies in der Vernehmlassungsversion des Vorentwurfs (Art. 32 VE-BÜPF) vorgesehen war. Für diese Lösung sprechen mehrere Gründe: Zunächst erhält der Dienst am ehesten von Vorkommnissen Kenntnis, die eine solche strafbare Handlung darstellen können. Auch bedroht Artikel 39 insbesondere die Nichtbefolgung der Anweisungen des Dienstes mit Strafe. Zudem überträgt das BÜPF dem Dienst Aufgaben im Bereich der administrativen Überwachung. Schliesslich erfordern die Verfolgung und Beurteilung dieser Straftaten spezifische technische Kenntnisse, über die der Dienst eher verfügen dürfte als die Strafverfolgungsbehörden der Kantone.

2.11 11. Abschnitt: Aufsicht und Rechtsschutz

Art. 41 Aufsicht

Es muss sichergestellt werden, dass auf dem Schweizer Markt nur jene dem BÜPF unterstellten Personen im Rahmen des Gesetzes tätig sein können, die sich an die Rechtsvorschriften zur Überwachung des Post- und Fernmeldeverkehrs halten. Dieses Ziel soll mit *Artikel 41* erreicht werden, der sich auf die administrative Beaufsichtigung der dem BÜPF unterstellten Personen bezieht und Artikel 58 FMG teilweise für sinngemäss anwendbar erklärt. Es wird ein System von administrativen Sanktionen eingeführt, das sich vom System der strafrechtlichen Sanktionen nach den Artikeln 39 f. unterscheidet und dieses ergänzt. Gegenüber den Mitwirkungspflichtigen (Art. 2), übt der Dienst seine Kompetenzen nach *Artikel 41* mit bindender Wirkung aus. Gegenüber den anordnenden Behörden und den Genehmigungsbehörden übt er hingegen diese Kompetenz ohne bindende Wirkung aus, da er ihnen gegenüber keine Entscheidungsbefugnis besitzt (siehe die Erläuterungen zu Art. 16 Bst. a und b).

Absatz 1 entspricht sinngemäss Artikel 58 Absatz 1 FMG. Im Bereich des Post- und Fernmeldeverkehrs übernimmt der Dienst die Rolle der Aufsichtsbehörde, da er die Materie und die geltenden Vorschriften am besten kennt.

Absatz 2 entspricht sinngemäss Artikel 58 Absatz 2 Buchstabe a FMG. Er enthält die Massnahmen, die der Dienst ergreifen kann, wenn er eine Rechtsverletzung betreffend die Überwachung des Post- und Fernmeldeverkehrs feststellt. In einer solchen Situation ermöglicht diese Bestimmung dem Dienst, eine Mahnung auszusprechen, damit ein festgestellter Mangel behoben wird oder geeignete Massnahmen zur Vorbeugung eines Wiederholungsfalls getroffen werden. Der Empfänger einer solchen Mahnung muss den Dienst über die getroffenen Massnahmen informieren. Der *zweite Satz von Absatz 2* entspricht sinngemäss Artikel 58 Absatz 5 FMG. Zusätzlich zur Mahnung kann der Dienst gestützt auf Artikel 40 strafrechtlich vorgehen. Wie dies bereits heute der Fall ist, können bei einer Verletzung der Rechtsvorschriften zur Überwachung des Post- und Fernmeldeverkehrs einschneidendere Massnahmen als jene verhängt werden, die nach *Absatz 2* in die Kompetenz des Dienstes fallen. In Bezug auf den Postverkehr obliegt es dem Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation, diese Massnahmen anzuordnen, während in Bezug auf den Fernmeldeverkehr das Bundesamt für Kommunikation und die Eidgenössische Kommunikationskommission zuständig

sind. Wie bisher können das Bundesamt für Kommunikation und die Eidgenössische Kommunikationskommission gestützt auf die Artikel 58 und 60 FMG handeln, und der Dienst kann diese Behörden über festgestellte Rechtsverletzungen informieren, damit sie nötigenfalls die aufgeführten Massnahmen anordnen können. Es ist nicht erforderlich, in Anlehnung an Artikel 58 Absatz 2 Buchstabe b FMG eine Bestimmung einzuführen, gestützt auf welche der Dienst eine Anbieterin von Fernmeldediensten verpflichten kann, den Betrag, den sie gespart hat, indem sie die angeordnete Überwachung nicht durchgeführt oder die Investitionen zur Erfüllung ihrer Pflichten im Überwachungsbereich nicht getätigt hat, an den Bund abzuliefern. Die Anbieterin kann in einem solchen Fall zwar Ausgaben vermeiden, sie erzielt damit aber keinen finanziellen Vorteil im Sinne der genannten Bestimmung. Sie muss jedoch die dem Dienst entstandenen Kosten gemäss Artikel 34 erstatten. Nach Artikel 33 Absatz 5 kann der Dienst die Anbieterin ausserdem anweisen, technische und organisatorische Massnahmen zu treffen, um die Mängel im Zusammenhang mit der Überwachung zu beheben. Schliesslich kann die Anbieterin strafrechtlich verfolgt werden, wenn sie der Anweisung des Dienstes zur Durchführung der angeordneten Überwachung oder der Anweisung nach Artikel 33 Absatz 5 nicht Folge leistet (Art. 39 Abs. 1 Bst. a).

Art. 42 Rechtsschutz

Einleitend ist festzuhalten, dass sich *Artikel 42* nicht auf den Rechtsschutz der Personen bezieht, die Gegenstand einer Überwachung des Post- oder Fernmeldeverkehrs bilden oder von einer solchen Überwachung betroffen sind; dieser ist in Artikel 279 Absatz 3 StPO oder 70*k* MStP geregelt. In Artikel 279 Absatz 1 StPO ist zudem geregelt, welche überwachten Drittpersonen nachträglich informiert werden müssen; es handelt sich dabei ausschliesslich um die Drittpersonen gemäss Artikel 270 Buchstabe b StPO. Weitere Betroffene, z.B. Personen, die mit der überwachten Person kommunizieren oder Personen, die im Rahmen eines Antennensuchlaufes oder beim Einsatz eines IMSI-Catchers vor der Filterung der Ergebnisse zwangsläufig ebenso erfasst werden, sind nicht von der Mitteilungspflicht nach Artikel 279 StPO betroffen und haben kein Beschwerderecht nach Absatz 3 der genannten Bestimmung. Dies ist auch sachgerecht, da diese Personen nicht im Sinne des Gesetzes überwacht werden. Die Artikel 269–279 StPO (insb. Art. 269–269ter StPO in der geänderten Fassung) regeln die strafprozessuale Zulässigkeit einer Überwachung abschliessend. So dürfen beispielsweise die Resultate einer Überwachung (in Echtzeit oder rückwirkend; Kommunikationsinhalte oder Randdaten) ohne Genehmigung durch ein Zwangsmassnahmengericht (oder das Militärkassationsgericht) nicht ausgewertet werden; nicht genehmigte Überwachungen werden sofort gestoppt und die gesammelten Daten vernichtet (Art. 277 StPO).

Die nach BÜPF Mitwirkungspflichtigen (Art. 2) sind von solchen strafprozessualen Fragen nur mittelbar betroffen, und zwar insofern sie eine Überwachung durchführen oder dulden müssen. Das BÜPF hat sich deshalb zu strafprozessualen Aspekten nicht zu äussern, sondern soll einzig und allein die technische Umsetzung der strafprozessual zulässigen Überwachungen sicherstellen (Notsuche und Fahndung nach verurteilten Personen vorbehalten). Nur in Bezug auf diese technische und verwaltungsrechtliche Seite ist es demzufolge nötig, den Rechtsschutz der in den Anwendungsbereich des BÜPF fallenden Personen hier zu regeln; diese Auffassung ent-

spricht im Übrigen auch der Lehre und der Rechtsprechung[69]. Personen die in den Geltungsbereich des BÜPF fallen, können demnach in einer verwaltungsrechtlichen Beschwerde keine strafprozessualen Gründe geltend machen. Die Gutheissung einer verwaltungsrechtlichen Beschwerde einer Fernmeldedienstanbieterin kann also nicht dazu führen, dass eine vom Zwangsmassnahmengericht genehmigte Überwachung aufgehoben wird, sondern nur dazu, dass eine Fernmeldedienstanbieterin eine Überwachung nicht selber durchführen muss, weil sie technisch oder organisatorisch nicht dazu in der Lage ist. Die Anbieterin ist jedoch verpflichtet, die Überwachung durch den Dienst oder Dritte zu dulden (Art. 26 Abs. 2) und den Dienst bei der Durchführung zu unterstützen (Art. 32 Abs. 2). Auch die Kostenfrage kann in einer verwaltungsrechtlichen Beschwerde aufgeworfen werden (siehe die Erläuterungen zu Art. 38).

Die klare Unterscheidung zwischen StPO und BÜPF ist sinnvoll, weil die beiden Erlasse – wie oben dargelegt – unterschiedliche Adressaten haben und unterschiedliche Regelungszwecke verfolgen (siehe auch die Erläuterungen zu Art. 31). Diese unterschiedlichen Regelungsbereiche wirken sich unmittelbar auch auf den Rechtsschutz aus. Die «Dualität» des Rechtsschutzes ist also eine Folge der Trennung der verwaltungsrechtlichen (BÜPF) von den strafprozessualen (StPO) Aspekten, die im Übrigen der Forderung in Ziffer 2 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision) entspricht.

In *Absatz 1* geht es demnach einzig um die Beschwerdemöglichkeit der Mitwirkungspflichtigen (Art. 2) und der Behörden, die dem Dienst Gebühren entrichten müssen, gegen die Verfügungen des Dienstes.

Bisher enthält das BÜPF keine Bestimmung zu Rechtsmitteln der Mitwirkungspflichtigen. Dies gilt sowohl allgemein (zum Beispiel in Bezug auf die Entschädigungen) als auch im Besonderen in Bezug auf Verfügungen des Dienstes, mit denen die Durchführung einer von der zuständigen Behörde angeordneten Überwachung verlangt wird. Nur in Artikel 32 der geltenden VÜPF wird diesen Personen das Recht zuerkannt, eine Verfügung des Dienstes anzufechten, mit der die Durchführung einer Überwachung verlangt wird. Diese Personen können sich im Rahmen einer derartigen Beschwerde jedoch – wie oben ausgeführt – nur auf technische oder organisatorische Fragen im Zusammenhang mit der Durchführung der von ihnen verlangten Überwachungsmassnahme berufen. Aus Gründen der Klarheit und Rechtssicherheit sieht der Entwurf nun eine Bestimmung vor, welche die Rechtsmittel der dem BÜPF unterstellten Personen gegen Verfügungen des Dienstes ausdrücklich regelt.

Etliche Vernehmlassungsteilnehmer kritisierten die vorgeschlagene Regelung (Art. 34 VE-BÜPF), die darauf hinauslaufe, dass der Beschwerdeführer die Rechtmässigkeit der vom Dienst übermittelten Überwachungsanordnung nicht durch ein Gericht überprüfen lassen könne. Diese Auffassung ist jedoch unzutreffend: Zum einen können die Verfügungen des Dienstes, soweit sie die technische und organisatorische Umsetzung der Überwachungsanordnung betreffen, nach Massgabe der allgemeinen Bestimmungen der Verwaltungsrechtspflege des Bundes überprüft

69 Thomas Hansjakob, a.a.O. (Fussnote 11), Art. 32 VÜPF N 3. BGE **130** II 249, E. 2.2.2 und 2.2.3. Vgl. auch BVGE 2009/46, E. 3.1.3, 3.2, 3.3 (Nichteintreten auf die Rüge der Fernmeldedienstanbieterin, die überwachte Person werde ohne gesetzliche Grundlage in ihren Rechten verletzt).

werden. Zum anderen wird die Frage der strafprozessualen Zulässigkeit im Strafverfahren nach den Regeln des Strafprozessrechts überprüft. Die Auffassung, das Bundesverwaltungsgericht müsse die strafprozessuale Zulässigkeit ebenso überprüfen können, würde die Rechtssicherheit nachhaltig gefährden: Die parallele Zuständigkeit liefe darauf hinaus, dass Entscheidungen des strafprozessualen Zwangsmassnahmengerichtes unter Nichteinhaltung des Instanzenzuges und in einem von der Rechtsordnung nicht vorgesehenen «Wechsel des Rechtsweges» widerrufen werden könnten. Umgekehrt wäre es denkbar, dass die Entscheidung des Bundesverwaltungsgerichtes über die strafprozessuale Rechtmässigkeit der Überwachungsanordnung eine Beschwerde der beschuldigten Person nach Artikel 279 Absatz 3 StPO aushebelt und diese so in ihren verfassungsmässigen Rechten verletzt.

Angesichts der allgemeinen Verfahrensregeln, die vor dem Bundesverwaltungsgericht gelten, kann der Beschwerdeführer diesem nur jene Rechtsfragen zur Überprüfung vorlegen, an deren Beantwortung er ein rechtlich geschütztes Interesse hat (Art. 37 des Bundesgesetzes vom 17. Juni 2005[70] über das Bundesverwaltungsgericht [VGG] in Verbindung mit Art. 48 Abs. 1 Bst. c VwVG). Daraus folgt, dass sich die Mitwirkungspflichtigen (Art. 2), insbesondere die Anbieterinnen von Fernmeldediensten, auf jeden Fall nicht auf Gründe berufen können, die das Strafverfahren oder den Schutz der Daten der kommunizierenden Personen betreffen. Ein Sachverhalt kann zwar Rechtsfragen aufwerfen, die sowohl das Strafprozessrecht als auch das Verwaltungsrecht (einschliesslich Datenschutzrecht) betreffen. So betrifft die Frage, ob ein Überwachungstyp (zum Beispiel der Antennensuchlauf) zulässig ist, sowohl das Strafprozess- und das Datenschutzrecht (darf der Staat die Benutzerinnen und Benutzer von Mobiltelefonen mittels Antennensuchlauf überwachen?) als auch das verwaltungsrechtliche Verhältnis zu den Anbieterinnen von Fernmeldediensten (müssen die Fernmeldedienstanbieterinnen Antennensuchläufe durchführen?). Mit Rücksicht auf die unterschiedliche Betroffenheit und die unterschiedlichen Fragestellungen dürfen diese Themen jedoch nicht vermischt werden; der Rechtsschutz ist vielmehr differenziert auszugestalten.

Die Beschwerdelegitimation der dem BÜPF unterstellten Personen, insbesondere der Anbieterinnen von Fernmeldediensten, ist somit für alle strafprozessualen Aspekte ausgeschlossen, da sie hier kein rechtlich geschütztes Interesse haben. Dies gilt etwa für die Frage, ob tatsächlich ein dringender Verdacht nach Artikel 269 Absatz 1 Buchstabe a StPO oder 70 Absatz 1 Buchstabe a MStP vorliegt oder ob die Voraussetzungen für die Überwachung des Fernmeldeanschlusses einer Drittperson nach Artikel 270 Buchstabe b StPO oder 70*a* Buchstabe b MStP gegeben sind. Diese Fragen wirken sich nur indirekt auf die Fernmeldedienstanbieterinnen aus.

In *Absatz 2* wird im Grunde nur ausdrücklich festgehalten, was oben dargelegt wurde und aufgrund der allgemeinen Verfahrensregeln auf jeden Fall gilt. Dennoch ist es sinnvoll, diese Bestimmung vorzusehen, da sie einen Punkt klarstellt, der für die Strafverfolgungs- und Verwaltungsrechtspraxis von Bedeutung ist.

Insbesondere angesichts der Dringlichkeit, die bei der Durchführung einer Überwachung regelmässig besteht, ist in *Absatz 3 erster Satz* vorgesehen, dass der Beschwerde keine aufschiebende Wirkung zukommt, ausser wenn die Verfügung des Dienstes eine Geldleistung betrifft (zum Beispiel Entschädigungen oder Gebühren), da davon auszugehen ist, dass in diesem Fall keine Dringlichkeit besteht.

70 SR **173.32**

Damit wird von Artikel 55 Absatz 1 VwVG abgewichen, der aufgrund des Verweises in Artikel 37 VGG an sich anwendbar wäre. Damit die Beschwerde keine aufschiebende Wirkung entfaltet, ist es folglich nicht notwendig, dass ihr der Dienst die aufschiebende Wirkung in Anwendung von Artikel 55 Absatz 2 VwVG entzieht. Wie dies Artikel 55 Absatz 3 VwVG vorsieht, ist jedoch in *Absatz 3 zweiter Satz* festgelegt, dass die Beschwerdeinstanz die aufschiebende Wirkung anordnen kann. Auch eine strafprozessuale Beschwerde hat grundsätzlich keine aufschiebende Wirkung hat (Art. 387 StPO), weil der Zweck der Überwachung darin besteht, Beweismittel zu beschaffen, was in der Regel keinen Aufschub duldet.

2.12 12. Abschnitt: Schlussbestimmungen

Art. 43 Vollzug

In *Artikel 43* ist vorgesehen, dass der Bundesrat für den Erlass der Vorschriften zum Vollzug des neuen BÜPF zuständig ist. Ebenfalls vorgesehen ist eine solche Zuständigkeit der Kantone, mit der insbesondere auf Artikel 37 Absatz 3 Bezug genommen wird.

Art. 44 Aufhebung und Änderung bisherigen Rechts

Im Anhang, auf den *Artikel 44* Bezug nimmt, ist in Ziffer I im Wesentlichen festgelegt, dass das Bundesgesetz vom 6. Oktober 2000[71] betreffend die Überwachung des Post- und Fernmeldeverkehrs mit dem Inkrafttreten des neuen BÜPF aufgehoben wird. Dies, weil mit dem neuen BÜPF das geltende BÜPF nicht geändert, sondern ersetzt wird.

In Ziffer II des Anhangs, auf den *Artikel 44* verweist, sind die Bundesgesetze aufgeführt, die mit dem Inkrafttreten des neuen BÜPF geändert, jedoch nicht aufgehoben werden.

Art. 45 Übergangsbestimmungen

Die Übergangsbestimmungen sind grundsätzlich darauf ausgerichtet, das bisherige Recht möglichst rasch durch das neue Recht zu ersetzen. Auf diese Weise sollen die Vorteile des neuen Rechts so schnell wie möglich zum Tragen kommen, weil das neue Recht im Vergleich zu den geltenden Bestimmungen als das bessere Recht beurteilt wird. Von diesen Übergangsbestimmungen erfasst werden Überwachungen nach diesem Gesetz (d.h. Überwachungen, die in Art. 269 StPO vorgesehen sind, aber auch durch das BÜPF geregelt werden) und die Beschwerden, die Überwachungen nach diesem Gesetz betreffen. Daraus ergibt sich die Abgrenzung gegenüber den Überwachungen, die ausschliesslich in der StPO geregelt sind (insbesondere Überwachungen mittels IMSI-Catchern [Art. 269bis StPO] und GovWare [Art. 269ter]), und den Beschwerden, die diese Überwachungen betreffen; diese Beschwerden sind somit Gegenstand der in der StPO vorgesehenen Übergangsbestimmungen sind.

71 AS **2001** 3096, **2003** 2133 3043, **2004** 2149 3693, **2006** 2197 5437, **2007** 921 5437

Absatz 1 orientiert sich an Artikel 448 Absatz 1 StPO, ohne dass die darin enthaltene Regelung genau übernommen wird. Gemäss der vorgeschlagenen Regelung wird für die Durchführung von Überwachungen das zum jeweiligen Zeitpunkt geltende Recht angewandt. Das neue Recht wird somit nicht zu einem Zeitpunkt angewandt, der vor seinem Inkrafttreten liegt. Dies gilt auch für Überwachungen, die noch im Gange sind. Mit dem Inkrafttreten des neuen Rechts kommt man somit nicht auf bereits durchgeführte Massnahmen zurück. In Übereinstimmung mit dem Rückwirkungsverbot ist das neue Recht selbstverständlich nicht auf Überwachungen anwendbar, die zum Zeitpunkt seines Inkrafttretens bereits durchgeführt wurden. Ist eine Überwachung im Gange, ist das neue Recht hingegen nach seinem Inkrafttreten auf die Strafverfolgung, auf die Weiterführung der Ermittlungen und auf die restliche Überwachung anwendbar. Damit besteht die Möglichkeit, die Vorteile des neuen Rechts bereits im jeweiligen Stadium zu nutzen, ohne dass die Durchführung der laufenden Untersuchung allzu stark kompliziert wird. Selbstverständlich ist das neue Recht auf Überwachungen anwendbar, die nach seinem Inkrafttreten angeordnet werden.

Absatz 2 orientiert sich an Artikel 453 Absatz 1 StPO, ohne dass die darin enthaltene Regelung genau übernommen wird. Beschwerden werden nach dem in erster Instanz anwendbaren Recht behandelt. Dies ist angesichts der Tatsache gerechtfertigt, dass in einem Beschwerdeverfahren abgeklärt werden soll, ob das Recht von der ersten Instanz richtig angewandt wurde.

Absatz 3 bezieht sich auf die Verlängerung der Aufbewahrungsfrist für die Randdaten des Post- und Fernmeldeverkehrs von sechs auf zwölf Monate. Randdaten, bei denen die im geltenden Recht geltende Aufbewahrungsfrist von sechs Monaten zum Zeitpunkt des Inkrafttretens des neuen Rechts noch nicht abgelaufen ist, müssen entsprechend dem neuen Recht während insgesamt zwölf Monaten aufbewahrt werden. Diese Frist läuft ab dem Beginn der Aufbewahrungsdauer nach dem geltenden Recht. *Im Umkehrschluss* müssen Randdaten, bei denen die im geltenden Recht geltende Aufbewahrungsfrist von sechs Monaten zum Zeitpunkt des Inkrafttretens des neuen Rechts abgelaufen ist, nicht länger aufbewahrt werden.

Absatz 4 bezieht sich auf die Aufhebung der Frist von zwei Jahren – die im geltenden BÜPF festgehalten ist – nach Aufnahme der jeweiligen Kundenbeziehung, während der die betreffenden Auskünfte verfügbar sein müssen. Auskünfte, bei denen die bisher geltende Frist von zwei Jahren zum Zeitpunkt des Inkrafttretens des neuen Rechts noch nicht abgelaufen ist, müssen gemäss dem neuen Recht unbefristet geliefert werden können. *Im Umkehrschluss* müssen Auskünfte, bei denen die bisherige Frist von zwei Jahren zum Zeitpunkt des Inkrafttretens des neuen Rechts abgelaufen ist, nicht mehr geliefert werden.

Absatz 5 enthält eine einfache Regelung: Anwendbar ist das Recht, das zum Zeitpunkt der Anordnung der Überwachung in Kraft gewesen ist. Der Zeitpunkt, zu dem eine (bereits angeordnete) Überwachung allenfalls verlängert wurde, spielt diesbezüglich keine Rolle. Dies bedeutet insbesondere, dass auf Entschädigungen und Gebühren für Überwachungen, die zum Zeitpunkt des Inkrafttretens des neuen Gesetzes bereits entrichtet werden, das alte Recht anwendbar ist.

Art. 46 Referendum und Inkrafttreten

Artikel 46 enthält die üblichen Bestimmungen zu Referendum und Inkrafttreten.

Strafprozessordnung[72]

Art. 269 Abs. 2 Bst. a

Die Erfahrung hat gezeigt, dass die aktuellen Instrumente – einschliesslich der Notsuche (Art. 35 E-BÜPF) – zur Lokalisierung eines widerrechtlich verbrachten oder zurückgehaltenen Kindes nicht ausreichen. Die Überwachung des Post- und Fernmeldeverkehrs, also eine Massnahme, die zur Lokalisierung eines Kindes beitragen kann, kann nicht angeordnet werden, weil der Tatbestand der Entziehung von Unmündigen (Art. 220 StGB) nicht im Katalog der überwachungsfähigen Straftaten aufgeführt ist. Aus diesem Grund muss *Artikel 269 Absatz 2 Buchstabe a* StPO mit einem Verweis auf Artikel 220 StGB ergänzt werden.

Art. 269bis (neu) Einsatz von besonderen technischen Geräten zur Überwachung des Fernmeldeverkehrs

Artikel 269bis bildet für die Staatsanwaltschaft die ausdrückliche gesetzliche Grundlage für den breiteren Einsatz von Überwachungsgeräten wie IMSI-Catchern, namentlich zur Identifikation mobiler Kommunikationsgeräte und mithin ihrer Benutzerinnen und Benutzer. Der Begriff «mobile Kommunikationsgeräte» umfasst nicht nur Mobiltelefone, sondern insbesondere auch Laptops und Notebooks mit SIM-Karten für die Übertragung von Daten über das Mobiltelefonnetz. Diese neue gesetzliche Grundlage bietet auch die Möglichkeit, IMSI-Catcher für das Abhören (und Aufzeichnen) der Kommunikation und für die Lokalisierung mobiler Kommunikationsgeräte und deren Benutzerinnen und Benutzer zu verwenden. Die Strafverfolgungsbehörden, die den IMSI-Catcher heute einsetzen, stützen sich auf Artikel 280 Buchstaben a und c StPO. Die Ergänzung ist für die Verfolgung von Straftaten notwendig. Zudem stellt die Identifikation im Vergleich zu den genannten Massnahmen der Ortung und des Abhörens von Gesprächen, die bereits in Artikel 280 StPO vorgesehen sind[73], einen weniger starken Eingriff in die Privatsphäre dar. Mit dem IMSI-Catcher lassen sich die Auswirkungen der Basisstation eines Mobiltelefonnetzes auf die Mobiltelefongeräte simulieren, die sich in seinem Sendebereich befinden. Dies hat zur Folge, dass sich die Mobiltelefongeräte beim betreffenden «IMSI-Catcher» anmelden und sich bei ihm identifizieren, wie sie dies bei irgendeiner Basisstation eines Mobiltelefonnetzes tun würden. Auf diese Weise lässt sich ohne jegliches Zutun der Telefondienstbetreiberin die bisher unbekannte Nummer der verwendeten Teilnehmer-Identifikationskarte (SIM-Nummer) oder internationale Identifikationsnummer (IMSI-Nummer oder IMEI-Nummer) einer bestimmten Person oder eines bestimmten Geräts identifizieren. Ausserdem lassen sich die Geräte in diesem Bereich orten und sogar die Telefongespräche abhören[74].

Eine verhältnismässig grosse Zahl der Vernehmlassungsteilnehmer, insbesondere Kantone und Organisationen im Bereich der Strafverfolgung, begrüsste die Schaffung einer gesetzlichen Grundlage, die den Einsatz von Überwachungsgeräten wie IMSI-Catchern im genannten Sinn ermöglicht. Abgelehnt wurde die Schaffung dieser Möglichkeit von der Grünen Partei der Schweiz, von Konsumentenschutzorganisationen sowie insbesondere von Organisationen von Internet-Benutzern. Zur

72 SR **312.0**
73 Sophie de Saussure, a.a.O., Rz. 45–56, 70.
74 Sylvain Métille, a.a.O., Rz. 25.

Untermauerung dieser Haltung wurde insbesondere geltend gemacht, IMSI-Catcher würden nicht nur die Identifikation des Mobiltelefons eines bestimmten Benutzers ermöglichen, sondern im entsprechenden Mobiltelefonnetz die Kommunikation aller – verdächtigen und unverdächtigen – Personen umleiten (und stören), die sich im Umkreis des abgehörten Benutzers aufhalten. Aufgeworfen wurde auch die Frage, ob die systematische Einordnung dieser Überwachungsmassnahme richtig ist (Art. 269 ff. StPO oder Art. 280 f. StPO).

Die systematische Einordnung des Einsatzes von Überwachungsgeräten wie IMSI-Catchern in der StPO entspricht der Forderung in Ziffer 2 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision), gemäss der alle Aspekte der Strafverfolgung aus dem BÜPF zu streichen sind. Unter dem Gesichtspunkt der Systematik beruht der Einsatz von Überwachungsgeräten wie IMSI-Catchern ausschliesslich auf Artikel 269 ff. StPO, und nicht auf Artikel 280 f. StPO. Die Anwendung dieser Überwachungsmethode erfordert zwar nach heutigem Stand keine Mitwirkung einer Fernmeldedienstanbieterin, und dem Dienst kommt beim Einsatz dieser Überwachungsgeräte auch keine besondere Aufgabe zu (er muss also keine Überwachungsanordnung erhalten). Es handelt sich jedoch um die Beschaffung von Daten des Fernmeldeverkehrs, weshalb die Bestimmung auch dort anzusiedeln ist[75].

Diese Überwachungsmethode muss insbesondere von jener Art der Überwachung unterschieden werden, bei der ein Antennensuchlauf durchgeführt wird. Dabei geht es darum, von den Anbieterinnen von Fernmeldediensten die Daten von Mobiltelefongesprächen zu erhalten, die während eines bestimmten Zeitraums über ihre Mobiltelefonnetze abgewickelt wurden, damit anhand der geografischen Koordinaten der genaue Standort des betreffenden Mobiltelefons bestimmt werden kann. Die beschafften Daten dienen somit dazu, den Ort zu ermitteln, an dem sich während des betrachteten Zeitraums ein Mobiltelefon und demzufolge auch dessen Benutzerin oder dessen Benutzer befunden haben. Es ist darauf hinzuweisen, dass für den Einsatz von technischen Überwachungsgeräten im Sinne von Artikel 269bis StPO, vorbehaltlich gegenteiliger Bestimmungen in diesem Artikel, die Artikel 269–279 StPO gelten. Dies bedeutet insbesondere, dass ein von der Staatsanwaltschaft angeordneter Einsatz eines IMSI-Catchers vom Zwangsmassnahmengericht genehmigt werden muss.

Aus *Buchstabe a* geht insbesondere hervor, dass die Straftaten, bei denen eine Überwachung des Fernmeldeverkehrs mittels Geräten wie dem IMSI-Catcher möglich ist, jenen entsprechen, bei denen eine klassische Überwachung nach Artikel 269 StPO zulässig ist.

In *Buchstabe b* ist vorgesehen, dass technische Überwachungsgeräte wie IMSI-Catcher wegen ihrer technischen Eigenschaften und insbesondere aufgrund der Tatsache, dass sie den Fernmeldeverkehr stören können, nur als subsidiäre Überwachungsinstrumente eingesetzt werden dürfen. Ihre Verwendung muss sich darauf beschränken, Lücken zu füllen, die im Bereich der heute verfügbaren klassischen Überwachungsmethoden bestehen. Sie sollten die aktuellen Instrumente für die Überwachung des Fernmeldeverkehrs im Sinne von Artikel 269 StPO nicht ersetzen[76].

75 Sophie de Saussure, a.a.O., Rz. 16, 20, 41–44; anderer Ansicht Sylvain Métille, a.a.O., Rz. 26, 40.
76 Sophie de Saussure, a.a.O., Rz. 72.

Da diese technischen Überwachungsgeräte den Fernmeldeverkehr stören können, ist in *Buchstabe c* festgelegt, dass solche Geräte nur eingesetzt werden dürfen, wenn vorgängig die erforderliche Genehmigung erteilt wurde. Diese Genehmigung, die nicht vom Zwangsmassnahmengericht, sondern vom Bundesamt für Kommunikation (BAKOM) ausgestellt wird, beruht auf den Artikeln 32*a* und 34 Absatz 1ter FMG, auf Artikel 6 Absatz 4 der Verordnung vom 14. Juni 2002[77] über Fernmeldeanlagen (FAV) und auf den Artikeln 49 ff. der Verordnung vom 9. März 2007[78] über Frequenzmanagement und Funkkonzessionen (FKV). In der Praxis muss die Behörde, die ein solches technisches Überwachungsgerät einsetzen will, für die Einholung der notwendigen Genehmigung ein entsprechendes Gesuch beim BAKOM einreichen. In diesem Gesuch müssen alle technischen Parameter des Geräts angegeben werden. Das BAKOM legt fest, ob die Voraussetzungen für die Erteilung einer Genehmigung erfüllt sind. Dabei geht es insbesondere um die Frage, ob durch die Verwendung des betreffenden Geräts unter dem Gesichtspunkt der Leistungsfähigkeit des Fernmeldeverkehrs nicht andere öffentliche Interessen oder die Interessen von Dritten in übermässiger Weise beeinträchtigt werden. Es überprüft somit, welches Störungspotenzial in Bezug auf den Fernmeldeverkehr, insbesondere hinsichtlich der Mobiltelefonnetze, mit dem Einsatz des betreffenden Geräts verbunden ist[79]. Die Genehmigungen des BAKOM werden einem bestimmten Anwender für die Benutzung einer festgelegten Zahl von Geräten eines ganz bestimmten Typs erteilt. Sobald die Genehmigung des BAKOM für das betreffende Gerät vorliegt, kann dieses im Rahmen von Überwachungen verwendet werden. Für den Einsatz des Geräts im Rahmen von weiteren Überwachungen muss nicht jedes Mal eine neue Genehmigung eingeholt werden.

Art. 269ter (neu) Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs

Artikel 269ter soll der Staatsanwaltschaft die Möglichkeit einräumen, im Rahmen von Strafverfahren unter ganz bestimmten Bedingungen die Verwendung von besonderen Informatikprogrammen, sogenannter Government Software (GovWare), anzuordnen. Dabei geht es darum, diese Informatikprogramme in ein Datenverarbeitungssystem einzuführen, um den Inhalt der Kommunikation und Randdaten abzufangen und zu lesen. Diese Aufgabe übernimmt die Polizei auf Anordnung der Staatsanwaltschaft. Dieses Verfahren erfordert somit keine Mitwirkung einer Anbieterin von Fernmeldediensten. Ausserdem kommt dem Dienst beim Einsatz von GovWare keine besondere Aufgabe zu, er muss also keine Überwachungsanordnung erhalten. Selbstverständlich wird das Informatikprogramm ohne Wissen der Besitzerin oder des Besitzers des Datenverarbeitungssystems eingeschleust. Als «Datenverarbeitungssystem» gilt jedes Gerät, das den Fernmeldeverkehr über das Telefonnetz oder auf einem anderen Weg ermöglicht, zum Beispiel mobile und andere Computer, Mobil- und Festnetztelefone sowie Tablet-Computer. Der Einsatz von GovWare erfolgt ausschliesslich im Rahmen eines Strafverfahrens; präventiv darf GovWare nicht verwendet werden. GovWare wird oft als «Trojaner» bezeichnet. Abgesehen von der Tatsache, dass GovWare im Gegensatz zu Trojanern zu einem rechtmässi-

77 SR **784.101.2**
78 SR **784.102.1**
79 Für weitere Einzelheiten zu den möglichen Störungen, die durch IMSI-Catcher verursacht werden, und zu den Genehmigungen des BAKOM, siehe Sophie de Saussure, a.a.O., Rz. 57–59.

gen Zweck, nämlich zur Kriminalitätsbekämpfung, eingesetzt wird, besteht das Ziel bei GovWare nicht darin, dass sich das betreffende Überwachungsprogramm verbreitet, während dies bei einem Trojaner der Fall sein kann. Beim Einsatz von GovWare geht es vielmehr darum, dass die Staatsanwaltschaft die Möglichkeit hat, ein bestimmtes Gerät bzw. eine bestimmte Person zu überwachen[80].

GovWare ist vor allem von Nutzen, um im Bereich der Internettelefonie Gespräche abzufangen (Voice over IP [VoIP]), insbesondere bei der Internettelefonie des Typs Peer-to-Peer[81]. Bei dieser Art von Telefonie sind die ausgetauschten und abgehörten Daten verschlüsselt, womit sie ohne den Einsatz von GovWare nicht lesbar wären und nicht direkt verwendet werden könnten. Diese Überwachungsmethode wird auch in jenen Fällen verwendet, in denen eine Kommunikation, auch wenn sie nicht verschlüsselt ist, ohne die betreffende Methode nicht abgehört werden könnte. Dies ist beispielsweise bei Instant Messaging der Fall, das von einem tragbaren Computer oder Mobiltelefon aus mit verschiedenen Prepaid-SIM-DATAS-Karten erfolgt. In diesen Fällen kann die unverschlüsselte Kommunikation nur abgefangen werden, wenn ein Programm in den tragbaren Computer oder in das Mobiltelefon eingeführt wird.

Mit GovWare kann technisch auf sämtliche Daten, beispielsweise auch auf alle privaten Informationen zugegriffen werden (z.B. Dokumente, Fotos), die in einem Computer gespeichert sind. Dabei handelt es sich um potenziell persönliche Daten. Mit GovWare sollen jedoch nur die Daten aus dem Fernmeldeverkehr (akustische und optische Daten), der auch den Internetverkehr umfasst, beschafft werden können; von besonderem Interesse sind die Daten im Zusammenhang mit der Internettelefonie und dem E-Mail-Verkehr, die demnach ebenso beschafft werden können (siehe auch die Erläuterungen zu Art. 1 Abs. 1 E-BÜPF). Mit dieser Einschränkung wird insbesondere die Online-Durchsuchung eines Datenverarbeitungssystems mittels GovWare juristisch ausgeschlossen.

In der Frage, ob der Einsatz von GovWare im oben erwähnten Sinn nach Artikel 280 StPO, insbesondere nach dessen Buchstaben a und b, zulässig ist, gehen die Meinungen auseinander[82]. In der Rechtslehre wird mehrheitlich die Auffassung vertreten, dass der Einsatz von GovWare in diesen Fällen nicht zulässig ist. Einige Autoren sind der Meinung, dass diese Art des Einsatzes von GovWare nur mit einer sehr weiten Auslegung von Artikel 280 StPO möglich wäre. Das Bundesgericht hat sich mit dieser Frage bislang nicht auseinandergesetzt. In diesem Zusammenhang ist darauf hinzuweisen, dass die Strafverfolgungsbehörden (Bund und Kantone) GovWare ganz vereinzelt gestützt auf die Strafprozessbestimmungen eingesetzt haben, die vor dem Inkrafttreten der StPO am 1. Januar 2011 galten, insbesondere auf der Grundlage von Artikel 66 Absatz 2 des Bundesgesetzes vom 15. Juni 1934 über die Bundesstrafrechtspflege und der ehemaligen kantonalen Strafprozessordnungen. Die BKP, die im Auftrag der BA und nach vorgängiger Genehmigung des Bundesstraf-

80 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 3.

81 Vgl. Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 7 und Sylvain Métille, a.a.O., Rz. 30.

82 Vgl. Annegret Katzenstein in: Niggli/Heer/Wiprächtiger (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011, Art. 280 StPO N 16; Thomas Hansjakob in: Donatsch/Hansjakob/Lieber (Hrsg.) Kommentar zur Schweizerischen Strafprozessordnung, Zürich/Basel/Genf 2010, Art. 280 N 2; Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 16, 30; Sylvain Métille, a.a.O., Rz. 37.

gerichts handelte, hat bei vier Verfahren, die sich auf verschiedene Kategorien von Straftaten bezogen, GovWare eingesetzt. Diese Bestimmungen waren darauf beschränkt, die Verwendung von technischen Überwachungsgeräten zu gestatten, ohne dass sie genaue Angaben zum Zweck des Einsatzes solcher Geräte enthielten. Sie boten indessen die Möglichkeit, den Einsatz von GovWare auf eine sehr weite Auslegung des Begriffs «technische Überwachungsgeräte» zu stützen, die jedoch weniger weit gefasst war als die Auslegung, die erforderlich wäre, um eine solche Überwachung auf Artikel 280 StPO zu stützen. Im Rahmen der Erarbeitung der StPO wurde jedoch die Auffassung vertreten, dass die besagten Bestimmungen dem Erfordernis der Bestimmtheit grundrechtseinschränkender Normen nicht genügten. Deshalb wurde versucht, dieses Problem mit der Verabschiedung von Artikel 280 StPO[83] zu beheben. Vor dem Hintergrund der obigen Ausführungen erscheint es notwendig, eine ausdrückliche gesetzliche Grundlage zu schaffen, wenn GovWare zu den oben genannten Zwecken eingesetzt werden soll. Dies erscheint zumal angezeigt, als eine solche Rechtsgrundlage als gesetzlicher Rechtfertigungsgrund (Art. 14 StGB) für ein Verhalten dienen muss, das grundsätzlich unter Artikel 143bis StGB (Unbefugtes Eindringen in ein Datenverarbeitungssystem) fallen würde.

In Bezug auf den Grundsatz, eine Bestimmung für die Überwachung des Fernmeldeverkehrs mittels GovWare einzusetzen, waren die Meinungen im Rahmen des Vernehmlassungsverfahrens geteilt. Etliche Kantone und Organisationen im Bereich der Strafverfolgung sprachen sich für diese Möglichkeit aus. Abgelehnt wurde der Einsatz von GovWare von der Grünen Partei der Schweiz, von Konsumentenschutzorganisationen sowie insbesondere von Organisationen von Internet-Benutzern. Grosse Vorbehalte brachten die meisten Anbieterinnen von Fernmeldediensten und viele Privatpersonen an. Es stellte sich insbesondere die Frage, ob diese Art von Überwachung zugelassen werden soll, da sie einer einschneidenden Massnahme entspricht und potenziell die Online-Durchsuchung des gesamten Computers ermöglicht. Es wurde auch die Auffassung geäussert, die Einführung solcher Programme in Computer sei mit zu hohen Risiken für die Informatiksicherheit (Schaffung einer Sicherheitslücke im System, die von Straftätern genutzt werden kann, «Wiederverwertung» von GovWare durch Kriminelle für missbräuchliche Zwecke, Risiken für die Sicherheit des Rechners der Privatperson, auf dem GovWare eingeschleust wird, Risiken für das gesamte Netzwerk) sowie für die Verlässlichkeit und Integrität der Beweismittel verbunden (beispielsweise Änderung eines Schriftstücks durch GovWare). Im Weiteren wurde geltend gemacht, es sei nicht im Voraus bekannt, wie GovWare mit den anderen Elementen eines Datenverarbeitungssystems agieren wird, in das ein Bundestrojaner eingeschleust wird. Die Einführung von GovWare in ein Datenverarbeitungssystem könne eine Infizierung durch Schadsoftware einer verhältnismässig grossen Zahl von Datenverarbeitungssystemen in der Schweiz und im Ausland zur Folge haben. In diesem Zusammenhang stelle sich die Frage nach der Haftung (insbesondere des Bundes) für den dadurch entstandenen Schaden. In Zweifel gezogen wurde auch die Wirksamkeit dieser Überwachungsart. Im Übrigen wurde die Auffassung vertreten, diese Überwachungsart dürfe angesichts ihrer besonderen Merkmale, insbesondere unter Berücksichtigung des damit verbundenen erheblichen Eingriffs in die Grundrechte der betroffenen Person, nur im Zusammenhang mit einigen der (schwersten) Delikte zur Anwendung gelangen, die in Artikel 269 Absatz 2 StPO aufgeführt sind. Aufgeworfen wurde auch die Frage, ob die

83 Botschaft vom 21. Dezember 2005 zur Vereinheitlichung des Strafprozessrechts, BBl **2006** 1251.

systematische Einordnung dieser Überwachungsmassnahme richtig ist (Art. 269 ff. StPO oder Art. 280 und 281 StPO).

Nach Auffassung der befragten Fachleute aus dem Polizeibereich sind die im Zusammenhang mit GovWare geäusserten Befürchtungen unbegründet. Die GovWare bleibe ständig unter der Kontrolle der Strafverfolgungsbehörden (Polizei, die der Staatsanwaltschaft unterstellt ist). Die GovWare wird auf Anordnung der Staatsanwaltschaft von der Polizei in das Zielgerät (Computer) eingeschleust, je nach Situation – auf verhältnismässig einfache Weise – auf physischem Weg direkt in das Gerät oder aus der Ferne, was schwieriger zu bewerkstelligen ist. Im ersten Fall begibt sich die Polizei in den Raum, in dem sich das Zielgerät befindet, während die Einschleusung im zweiten Fall zum Beispiel über E-Mail erfolgt. Dabei muss unter Umständen ein Virenschutzprogramm umgangen werden. Gemäss den Anordnungen der Staatsanwaltschaft und entsprechend der Art der Informationen, die sie erhalten möchte (zum Beispiel Internettelefonie, nicht jedoch die besuchten Websites oder die Bilder, die mit der Kamera des Computers aufgenommen werden), wird die betreffende GovWare speziell für den Zielcomputer konzipiert und konfiguriert. Aufgrund dieser auf jeden Einzelfall abgestimmten Konfiguration ist der Einsatz von GovWare ein komplexes Unterfangen und ausserordentlich kostenintensiv. Für einen effizienten und zielgerichteten Einsatz von GovWare sind in der Regel vorgängig die Durchführung einer klassischen Überwachung des Fernmeldeverkehrs nach Artikel 269 StPO sowie eine Analyse des sozialen Umfelds der Zielperson erforderlich (vor allem in jenen Fällen, in denen ein bestimmter Internetanschluss von mehreren Personen benutzt wird). Damit soll verhindert werden, dass bei der Überwachung des Fernmeldeverkehrs der Zielperson weitere Personen in die Überwachungsmassnahmen einbezogen werden. GovWare diene somit genau und ausschliesslich jenen Zwecken, für die sie programmiert wurde. Sie übermittelt die Daten, die über den Fernmeldeanschluss der überwachten Person abgefangen werden, auf einen von den Strafverfolgungsbehörden verwendeten Server. Die Polizei, die unter der Aufsicht der Staatsanwaltschaft operiert, kann die GovWare auf dem Zielcomputer aktivieren. Mit der erforderlichen gerichtlichen Genehmigung, die von einem Zwangsmassnahmengericht ausgestellt wird, kann sie die Verwendung eines solchen Programms verlängern. Sofern keine automatische Deaktivierung vorgesehen wurde, hat die Polizei auch die Aufgabe, die GovWare zu deaktivieren. Alle diese Massnahmen werden vorgenommen, ohne dass sich die GovWare verbreitet. Ebenfalls unter der Aufsicht der Staatsanwaltschaft und mit einer Genehmigung des Zwangsmassnahmengerichts kann die Polizei eine laufende Überwachung gegebenenfalls nicht mehr ausschliesslich auf die ursprünglich überwachten Daten beschränken, sondern auf andere Arten von Daten ausweiten. Die Funktionsweise von GovWare hängt von ihrer Konfiguration ab; sie muss deshalb so konfiguriert werden, dass sie nur die Beschaffung von Fernmeldeverkehrsdaten ermöglicht, sodass kein Zugang zu sämtlichen Daten besteht, die im betreffenden Computer enthalten sind. Damit soll die Durchführung einer Online-Durchsuchung dieses Computers ausgeschlossen werden. Ein externes Unternehmen, das die GovWare konfiguriert hat, sei aus diesem Grund allein noch nicht in der Lage, auf die während einer Überwachung gesammelten Daten zuzugreifen. Die Person, die den Server verwaltet, der von der Strafverfolgungsbehörde für die Durchführung einer Überwachung mittels einer GovWare verwendet wird, könne deshalb die registrierten Daten nicht lesen. Sie könne lediglich die Übertragung dieser Daten feststellen. Aufgrund ihrer speziellen Merkmale und insbesondere der Tatsache, dass die GovWare speziell auf das Zielgerät abgestimmt wird und ihre Benutzung zeitlich beschränkt ist,

sei es sehr schwierig, die GovWare in diesem Computer zu kopieren und in einen anderen Rechner einzuschleusen. Das widerrechtliche Aneignen einer GovWare würde umfangreiche Kenntnisse und einen grossen Zeitaufwand erfordern. Für eine Person mit bösen Absichten sei es zudem viel einfacher, sich zu einem bescheidenen Betrag auf dem Markt einen Trojaner zu beschaffen. Im Übrigen stelle der Einsatz von GovWare für die Netzwerke kein Risiko dar, da dadurch keine Komponenten von Netzwerken betroffen seien.

Aus Sicht der kontaktierten Fachleute aus dem wissenschaftlichen Bereich ist es jedoch nicht möglich, GovWare zu entwickeln und in Betrieb zu halten, die unter allen Umständen korrekt funktioniert, d.h. keinen Einfluss auf andere Programme oder Funktionen hat. Laut Angaben dieser Fachleute geht indessen aus Versuchen hervor, dass es möglich ist, derartige Programme zu benutzen, ohne dass sofort feststellbare Schäden auftreten. Die von den Strafverfolgungsbehörden eingesetzte Software lasse sich technisch wohl (noch) nicht auf die Überwachung der Kommunikation allein beschränken: Die Hintertür, welche die GovWare öffnet, ermögliche den Ermittlern technisch den Zugriff auf sämtliche Daten und Informationen auf dem betroffenen Computersystem: Es könnten beliebige System- und Nutzerdaten ohne Wissen des Inhabers kopiert, verändert, gelöscht oder hinzugefügt werden. Diese Hintertür führe zudem zu einer Schwachstelle im Computersystem, welche auch von Dritten ausgenützt werden könne[84].

Das vorrangige Ziel der Revision des BÜPF besteht nicht darin, vermehrt zu überwachen, sondern die Überwachungsmethoden an die technische Entwicklung im Fernmeldebereich anzupassen. Dieses Ziel lässt sich nach Ansicht des Bundesrates nur erreichen, wenn den Strafverfolgungsbehörden gestattet wird, GovWare einzusetzen. Andernfalls würde die Wirksamkeit der Kriminalitätsbekämpfung sehr stark beeinträchtigt. Die Verschlüsselung, welche die Fernmeldedienstanbieterinnen nicht verhindern können, verunmöglicht die Überwachung mit klassischen Überwachungsmethoden, da die auf diese Weise gesammelten Daten nicht lesbar sind. Insbesondere auch im Bereich der Internettelefonie, die zunehmend an die Stelle der klassischen Telefonie tritt, wird eine solche Verschlüsselung bereits heute verwendet. Vielen Straftätern sind diese Schwachstellen im Bereich der Überwachung der Internettelefonie bekannt. Aus diesem Grund wickeln sie ihre telefonische Kommunikation über das Internet ab. Mit GovWare kann dieses Problem behoben werden. Statt die Daten während ihrer Übermittlung umzuleiten, wie dies bei den klassischen Massnahmen zur Überwachung des Fernmeldeverkehrs der Fall ist, wird mit GovWare versucht, die Daten an der Quelle abzufangen, also bevor sie verschlüsselt werden[85]. Mit den IPv6-Adressen werden in den nächsten Jahren allmählich neue Adressierungsressourcen eingeführt. Dies wird die Überwachung des Internetverkehrs, zu dem auch die Internettelefonie gehört, mit den klassischen Massnahmen der Fernmeldeüberwachung nach Artikel 269 StPO zunehmend erschweren oder gar verunmöglichen, da mit diesem neuen System der Einsatz von Verschlüsselungsprotokollen wie IPSec erleichtert wird. Ausserdem besteht gegenwärtig ein verstärkter Trend zur verschlüsselten Kommunikation (z.B. https). Daraus geht hervor, dass sich die Verschlüsselung zunehmend verbreiten wird. Mit dem Einsatz von

84 Vgl. zum Ganzen Sabine Gless, Strafverfolgung im Internet, in: Schweizerische Zeitschrift für Strafrecht, Band 130 [2012], S. 12, 17 f. und Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011 Rz. 2 f. (insb. Fn. 5), 10.

85 Für Einzelheiten siehe Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 5–9.

GovWare lässt sich verhindern, dass die Strafverfolgung durch die Nutzung des Internets und die Datenverschlüsselung ausgehebelt wird. Es lässt sich also folgende Schlussfolgerung ziehen: Wird den Strafverfolgungsbehörden nicht die Möglichkeit gegeben, GovWare einzusetzen, so wird die Überwachung der Internettelefonie und allgemein des Internetverkehrs sehr stark eingeschränkt. Es würden Massnahmen zur Überwachung des Internetverkehrs in Zukunft verhindert, die heute möglicherweise technisch noch machbar sind. Dies stünde jedoch klar im Gegensatz zum oben erwähnten Ziel der laufenden Revision des BÜPF.

Unter Berücksichtigung der obigen Ausführungen und nach einer Abwägung der verschiedenen Interessen hat der Bundesrat beschlossen, im vorliegenden Entwurf die Schaffung einer ausdrücklichen gesetzlichen Grundlage für die Verwendung von GovWare durch die Strafverfolgungsbehörden zu beantragen. Es wird vorgeschlagen, den Einsatz von GovWare einzig bei Ermittlungen wegen den in Artikel 286 Absatz 2 StPO katalogisierten Straftatbeständen zu erlauben, und nicht bei Ermittlungen gemäss dem umfassenderen Katalog von Artikel 269 Absatz 2, welcher bei den klassischen Überwachungsmassnahmen zur Anwendung gelangt (vgl. Abs. 1 Bst. b und die entsprechende Kommentierung). Der Bundesrat schlägt zudem vor, dass der Einsatz von GovWare nur subsidiär zu den klassischen Überwachungsmassnahmen erfolgen darf; der Grundsatz der Verhältnismässigkeit bleibt vorbehalten (vgl. Abs. 1 Bst. c und die entsprechende Kommentierung). Die Beschränkung der Überwachung auf Kommunikationsdaten muss juristisch sichergestellt werden. Die vorgeschlagenen Regeln sollen dies sicherstellen, indem «Inhalt der Kommunikation und Randdaten» als sachlicher Anwendungsbereich der GovWare genannt werden; die Online-Durchsuchung soll klar verboten sein[86]. Ausgeschlossen ist auch der Einsatz einer GovWare, um die Kamera oder das Mikrofon eines Computers zu einem anderen Zweck als zur Überwachung des Fernmeldeverkehrs zu nutzen (siehe Abs. 3 und die entsprechenden Erläuterungen). Es bestehen zudem starke gesetzliche Garantien, um betroffene Personen vor potenziellem Missbrauch im Zusammenhang mit dem Einsatz von GovWare zu schützen. So ist vorgesehen, für den Einsatz von GovWare zu Überwachungszwecken die Genehmigung der zuständigen Behörde (Zwangsmassnahmengericht) zu verlangen (Art. 274 StPO). Überdies können Informationen, die unter Verletzung der geltenden Einschränkungen gesammelt werden, zum Beispiel im Rahmen einer Online-Durchsuchung und nicht im Zusammenhang mit Daten, die ausschliesslich aus dem Fernmeldeverkehr stammen, keinesfalls als Beweismittel herangezogen werden und müssen vernichtet werden (Abs. 3 sowie Art. 141 Abs. 1 und 277 StPO). Zudem kann die betroffene Person gegen die ihr gegenüber angeordneten Überwachung mittels GovWare Beschwerde einlegen (Art. 279 StPO).

Der Einsatz von GovWare im oben erläuterten Sinn ist den theoretisch denkbaren Alternativen vorzuziehen, mit denen grundsätzlich das gleiche Ziel erreicht werden könnte: Analog zur Verpflichtung, der die Anbieterinnen von Fernmeldediensten unterstehen, könnte für die Internetdienstanbieterinnen wie beispielsweise aus dem Bereich der Internettelefonie die Verpflichtung vorgesehen werden, den Strafverfolgungsbehörden über den Dienst die Daten, insbesondere Kommunikationsdaten, von Personen zu liefern, die ihr Programm benutzen, um über das Internet zu telefonieren. Doch in der Praxis wäre es äusserst schwierig oder sogar unmöglich, eine solche Verpflichtung durchzusetzen. Denn mit der Einführung einer derartigen Verpflich-

86 Vgl. Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 21.

tung würde insbesondere nicht berücksichtigt, was von solchen Anbietern typischerweise zur Verfügung gestellt wird: Konkret umfasst ein solches Angebot üblicherweise ein Programm, das im Internet kostenlos heruntergeladen werden kann und mit dem über das Internet mit Hilfe von Verbindungen von Computer zu Computer (Peer-to-Peer) verschlüsselt telefoniert werden kann. Diese Internettelefonie-Verbindungen erfolgen nicht über eine von der jeweiligen Internetdienstanbieterin betriebene Zentrale. Dies bedeutet, dass die betreffende Internetdienstanbieterin nicht im Besitz der oben erwähnten Daten ist und diese somit den Strafverfolgungsbehörden nicht liefern kann. Mit der oben aufgeführten Verpflichtung würde im Weiteren die Tatsache ausser Acht gelassen, dass die grosse Mehrheit der Internetdienstanbieterinnen dieses Typs ihren Sitz im Ausland hat, womit die Durchsetzung der Verpflichtung illusorisch wäre. Eine andere Alternative zum Einsatz von GovWare würde darin bestehen, dass alle Unternehmen, welche die Verschlüsselung des Fernmeldeverkehrs ermöglichen, verpflichtet würden, ihre Verschlüsselungsalgorithmen herauszugeben, damit der betreffende Fernmeldeverkehr entschlüsselt werden kann. Mit dieser Verpflichtung würde aber ebenfalls nicht berücksichtigt, dass diese Internetdienstanbieterinnen ihren Sitz mehrheitlich im Ausland haben, womit die Durchsetzung auch bei dieser Verpflichtung illusorisch wäre.

Die Regelung des Einsatzes von GovWare in der StPO und nicht im BÜPF entspricht der Forderung in Ziffer 2 der Motionen Schmid-Federer 10.3831 (BÜPF-Revision), Eichenberger 10.3876 (BÜPF-Revision) und (von Rotz) Schwander 10.3877 (BÜPF-Revision), gemäss der alle Aspekte der Strafverfolgung aus dem BÜPF zu streichen sind. Für die systematische Verortung innerhalb der StPO kommen der Abschnitt «Überwachung des Post- und Fernmeldeverkehrs» (Art. 269 ff.) und der Abschnitt «Überwachung mit technischen Überwachungsgeräten» (Art. 280 f.) in Frage. Folgende Überlegungen sind ausschlaggebend: Beim Einsatz von GovWare wird zwar in das betreffende Datenverarbeitungssystem (Computer) eingedrungen und dieses manipuliert, was bei den Überwachungsmassnahmen nach Artikel 269 StPO gerade nicht der Fall ist, weil diesfalls Daten während ihrer Übertragung lediglich «umgeleitet» oder bei einer (Fernmelde-)Dienstanbieterin beschafft werden. Beim Einsatz von GovWare ist zwar keine Mitwirkung einer Fernmeldedienstanbieterin erforderlich und dem Dienst kommt hier keine besondere Aufgabe zu; trotzdem muss die gesetzliche Grundlage unter systematischen Gesichtspunkten in die Artikel 269 ff. StPO und nicht in die Artikel 280 f. StPO integriert werden, weil der Einsatz von GovWare ausschliesslich auf die Überwachung des Fernmeldeverkehrs beschränkt werden soll und beispielsweise die Raumüberwachung mit der Kamera des Computers nicht umfassen darf. Es ist zu präzisieren, dass für den Einsatz von GovWare im Sinne von Artikel 269ter StPO unter Vorbehalt der darin enthaltenen gegenteiligen Bestimmungen die Artikel 269–279 StPO gelten.

Absatz 1 Buchstabe a verweist nicht auf Artikel 269 Absatz 2 StPO, da die Straftaten, bei denen eine Überwachung des Fernmeldeverkehrs mittels GovWare möglich ist, nicht jenen entsprechen, bei denen eine klassische Überwachung nach Artikel 269 StPO zulässig ist (siehe Bst. b und die entsprechenden Erläuterungen).

Angesichts der Merkmale des Einsatzes von GovWare, insbesondere des sehr starken Eingriffs, den diese Überwachungsart darstellt, wird unter Berücksichtigung einiger kritischer Anmerkungen, die während des Vernehmlassungsverfahrens geäussert wurden, Folgendes vorgeschlagen: Im Gegensatz zur Regelung, die im Vernehmlassungsentwurf vorgesehen war, darf GovWare nur bei jenen Straftaten

eingesetzt werden, die in der Liste in Artikel 286 Absatz 2 StPO aufgeführt sind, welche sich auf die verdeckte Ermittlung bezieht. Der umfangreichere Deliktskatalog in Artikel 269 Absatz 2 StPO, der für die klassischen Überwachungen des Post- und Fernmeldeverkehrs gilt, gelangt dabei nicht zur Anwendung. Diese in *Absatz 1 Buchstabe b* formulierte Beschränkung ist jedoch nicht unumstritten. Diesbezüglich wird insbesondere geltend gemacht, der Eingriff in die Grundrechte der betroffenen Person sei bei einer Überwachung mittels GovWare einschneidender als bei einer Überwachung mit Hilfe des konventionellen Verfahrens, d.h. über eine Anbieterin von Fernmeldediensten nach den Artikeln 269 ff. StPO. In jenen Fällen, in denen sich der Einsatz von GovWare als notwendig erweist, sollte der obigen Tatsache nicht mit dieser Beschränkung Rechnung getragen werden. Es wird die Auffassung vertreten[87], stattdessen solle dieser Umstand bei der Anwendung des Grundsatzes der Verhältnismässigkeit nach Artikel 269 Absatz 1 Buchstabe b StPO berücksichtigt werden. Wenn im Rahmen einer Überwachung mittels GovWare Informationen zu Straftaten beschafft werden, die im Deliktskatalog in Artikel 269 Absatz 2 StPO, jedoch nicht in der Liste in Artikel 286 Absatz 2 StPO enthalten sind, hat die oben erwähnte Beschränkung insbesondere zur Folge, dass diese Informationen nicht ausgewertet werden können (Art. 141 Abs. 1 und 278 StPO).

Ebenfalls angesichts der oben erwähnten Merkmale des Einsatzes von GovWare wird in *Absatz 1 Buchstabe c* festgelegt, dass GovWare subsidiär zu den klassischen Massnahmen zur Überwachung des Fernmeldeverkehrs nach Artikel 269 StPO eingesetzt wird. Diese werden bereits subsidiär zu den klassischen Untersuchungsmassnahmen eingesetzt (Art. 269 Abs. 1 Bst. c StPO). Im Übrigen muss selbstverständlich der Grundsatz der Verhältnismässigkeit gewahrt bleiben (Art. 269 Abs. 1 StPO). Auf diese Weise kann gewährleistet werden, dass dieses Überwachungsverfahren nur zum Einsatz kommt, wenn dies wirklich notwendig ist. Die hohen Kosten für den Einsatz von GovWare werden zudem vermutlich dazu führen, dass von dieser Ermittlungsmethode nur mit Zurückhaltung Gebrauch gemacht wird. In diesem Zusammenhang ist darauf hinzuweisen, dass aus praktischen Gründen zuerst eine klassische Massnahme zur Überwachung des Fernmeldeverkehrs durchgeführt werden muss, um einen wirksamen Einsatz von GovWare zu ermöglichen.

Gemäss *Absatz 2 Buchstabe a* ist die Staatsanwaltschaft verpflichtet, in ihrer Überwachungsanordnung den gewünschten Datentyp zu bezeichnen. Diese Pflicht trägt dazu bei, dass die Einhaltung des folgenden Verbots (durch das Zwangsmassnahmengericht) kontrolliert wird: Es ist untersagt, andere Daten als jene zu beschaffen, die ausschliesslich aus dem Fernmeldeverkehr[88] stammen. Dies gilt insbesondere für Online-Durchsuchungen (siehe Abs. 3 und die entsprechenden Erläuterungen).

Gemäss *Absatz 2 Buchstabe b* ist die Staatsanwaltschaft auch verpflichtet, in ihrer Überwachungsanordnung anzugeben, ob es notwendig ist, zum Einführen von Informatikprogrammen in das betreffende Datenverarbeitungssystem in einen nicht öffentlichen Raum einzudringen. Diese Verpflichtung der Staatsanwaltschaft hat den Zweck, das Zwangsmassnahmengericht auf diese Ausführungsmodalität aufmerksam zu machen, damit es sie gemäss Artikel 274 Absatz 4 Buchstabe c StPO gegebenenfalls ausdrücklich genehmigen kann (siehe auch die Erläuterungen zu Art. 274 Abs. 4 Bst. c StPO).

87 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 25.
88 Sylvain Métille, a.a.O., Rz. 33, 38.

Nach *Absatz 3* ist insbesondere die Verwertung von Beweisen ausgeschlossen, die durch die Online-Durchsuchung eines Datenverarbeitungssystems mittels einer GovWare erhalten werden, mit der auf alle potenziell persönlichen Daten im System zugegriffen werden kann. Ausgeschlossen ist auch die Verwertung von Beweisen aus dem Einsatz einer GovWare, der erfolgte, um die Kamera oder das Mikrofon eines Computers zu einem anderen Zweck als zur Überwachung des Fernmeldeverkehrs zu nutzen, zum Beispiel zur Überwachung eines Raums. Die Verwendung von GovWare ist nach Absatz 1 ausschliesslich für die Beschaffung von Daten des Fernmeldeverkehrs erlaubt. Eine Online-Durchsuchung scheint grundsätzlich schon angesichts von Artikel 247 StPO ausgeschlossen zu sein, gemäss dem die betroffene Person über eine Durchsuchung in Kenntnis gesetzt werden muss. Der Einsatz von GovWare ergibt jedoch nur Sinn, wenn er ohne Wissen der betreffenden Person erfolgt. Gemäss Absatz 2 Buchstabe a ist die Staatsanwaltschaft verpflichtet, in ihrer Überwachungsanordnung den Typ der zu beschaffenden Daten zu bezeichnen. Diese Pflicht trägt dazu bei, die Einhaltung des folgenden Verbots zu kontrollieren: Es ist untersagt, insbesondere im Rahmen einer Online-Durchsuchung, andere Daten als jene zu beschaffen, die ausschliesslich aus dem Fernmeldeverkehr stammen[89]; Daten, die unter Verletzung dieses Verbots beschafft werden, dürfen nicht verwertet werden (Art. 141 Abs. 1 und 277 StPO)[90].

Mit dem Postulat der Kommission für Rechtsfragen des Nationalrates 11.4042 (Überwachung mittels Trojanern [1]) wurde der Bundesrat beauftragt, die Notwendigkeit einer Anpassung der Regelung zum Einsatz von GovWare zu prüfen und einen Bericht zu dieser Thematik vorzulegen. Mit dem Postulat der Kommission für Rechtsfragen des Nationalrates 11.4043 (Überwachung mittels Trojanern [2]) wurde der Bundesrat beauftragt, einen Bericht über den Einsatz von elektronischen Überwachungsinstrumenten, insbesondere von Trojanern, über die rechtlichen Grundlagen und über die Rahmenbedingungen des Einsatzes zu verfassen. Dieser Bericht soll die Situation beim Bund und, wenn möglich, auch bei den Kantonen darlegen. In den vorstehenden Ausführungen sind die in diesen Postulaten formulierten Forderungen berücksichtigt.

Art. 270 Einleitungssatz und Bst. b Ziff. 1

Im *Einleitungssatz* und in *Buchstabe b Ziffer 1* erfolgen terminologische Anpassungen in Übereinstimmung mit den im Entwurf BÜPF neu verwendeten Begriffen. Der Begriff «Anschluss» wird somit – je nach Kontext – durch den Begriff «Dienst» oder den Begriff «Verkehr» ersetzt (siehe die Erläuterungen zu Art. 17 E-BÜPF).

Der geltende französische Wortlaut erfasst nur die Entgegennahme von Sendungen und Mitteilungen durch die beschuldigte Person über die Postadresse oder den Fernmeldedienst einer Drittperson. Diese Fassung ist zu restriktiv. Wie im deutschen und im italienischen Wortlaut muss auch der Versand von Sendungen und Mitteilungen durch die beschuldigte Person über die Postadresse oder den Fernmeldeanschluss einer Drittperson erfasst werden. Daher wird der französische Wortlaut entsprechend angepasst.

89 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, Rz. 21; Sylvain Métille, a.a.O., Rz. 35, 40.
90 Sylvain Métille, a.a.O., Rz. 33, 38.

Art. 271

Artikel 271 wird genauer formuliert und ergänzt.

Es wird vorgeschlagen, anstelle der Vernehmlassungsversion von *Absatz 1* die geltende Fassung beizubehalten und diese zu ergänzen (vgl. unten). Denn die bestehende Formulierung ist klar, während aus der Vernehmlassungsversion geschlossen werden könnte, dass selbst jene Daten, die nicht ausgesondert wurden, von den Strafverfolgungsbehörden nicht verwertet werden dürfen. Die Aussonderung der Daten kann unter der Leitung eines Gerichts unter Verwendung technischer Massnahmen erfolgen, die es beispielsweise ermöglichen, nur den Verkehr mit ausgewählten Teilnehmerinnen und Teilnehmern bzw. Anschlüssen aufzubewahren. Es besteht kein Grund, in der Akte Informationen aufzubewahren, die in keinem Zusammenhang mit den Ermittlungen stehen und die dem Berufsgeheimnis unterstehen. *Absatz 1* muss daher ergänzt werden: Wie in Absatz 3 muss vorgesehen werden, dass diese Informationen vernichtet werden müssen und dass sie nicht verwendet werden dürfen.

Absatz 2 entspricht im Wesentlichen dem geltenden Absatz 2. Allerdings wird der Fall, auf den sich dieser Absatz bezieht, logischer dargelegt. Es wird dem Umstand Rechnung getragen, dass *Absatz 2* als Ausnahme in Bezug auf Absatz 1 zu betrachten ist, der den Grundsatz der Aussonderung festhält. Wenn die kumulativen Voraussetzungen von Absatz 2 erfüllt sind, muss die in Absatz 1 erwähnte Aussonderung nicht vorgenommen werden. Dies bedeutet in diesem Fall, dass zum einen die Strafverfolgungsbehörden direkt auf die Informationen zugreifen können, die im Rahmen der durchgeführten Überwachung gesammelt wurden, und dass zum anderen die betreffende Überwachung durch eine Direktschaltung vorgenommen werden kann. Denn aufgrund der Merkmale der Direktschaltung – dieser Begriff ist nicht mit der Echtzeit-Überwachung zu verwechseln – ist eine Aussonderung nach Absatz 1 nicht möglich. Siehe im Übrigen Artikel 17 Buchstabe c E-BÜPF und die entsprechenden Erläuterungen. In diesem Zusammenhang ist darauf hinzuweisen, dass nach dem Wortlaut von *Absatz 2 Buchstabe a* eine Direktschaltung nur möglich ist, wenn die Trägerin oder der Träger des Berufsgeheimnisses als beschuldigte Person überwacht wird, nicht jedoch, wenn sie oder er nach Artikel 270 Buchstabe b StPO als Drittperson überwacht wird. Im Vernehmlassungsverfahren wurde zu Recht darauf hingewiesen, dass das Interesse der Kunden, Patienten usw. am Geheimnisschutz im Fall von *Absatz 2* ebenso besteht wie in den Fällen nach den Absätzen 1 und 3. Da *Absatz 2* einen Sonderfall der Situation betrifft, die unter Absatz 1 fällt, dürfen die Informationen, die nicht mit den Ermittlungen zusammenhängen und die dem Berufsgeheimnis unterstehen, nicht in den Akten aufbewahrt werden; nach Absatz 1 müssen diese Informationen vernichtet werden, und ihre Auswertung ist untersagt.

Absatz 3 wird ergänzt, damit er die realen Abläufe besser widerspiegelt. Wie dies in Absatz 1 vorgesehen ist, muss verhindert werden, dass den Strafverfolgungsbehörden Informationen zur Kenntnis gelangen, die unter das Berufsgeheimnis fallen. Die Aussonderung, die unter der Leitung eines Gerichts erfolgen muss, betrifft ausschliesslich Informationen aus Sendungen und aus der Kommunikation mit den Personen, die in den Artikeln 170–173 genannt werden. Die Informationen aus der

Kommunikation mit Personen ohne diese Eigenschaft müssen nicht ausgesondert werden[91].

Art. 272 Abs. 2 erster Satz und Abs. 3

Terminologische Anpassungen, siehe dazu die Erläuterungen zu Artikel 270 Einleitungssatz und Buchstabe b Ziffer 1.

Art. 273 Teilnehmeridentifikation, Standortermittlung und technische Merkmale des Verkehrs

Die *Sachüberschrift* dieser Bestimmung wird geändert, damit sie mit deren Inhalt übereinstimmt.

Der in *Absatz 1* enthaltene Begriff Randdaten wird gegenüber dem heute geltenden Begriff vereinfacht, ohne dass sich der materielle Inhalt des Begriffs verändert (siehe die Erläuterungen zu Art. 19 Abs. 1 Bst. b und 26 Abs. 1 Bst. b E-BÜPF). Es ist darauf hinzuweisen, dass die Auskunft zur Dauer des Verkehrs («wie lange») letztlich nur für den Fernmeldeverkehr, jedoch nicht für den Postverkehr von Bedeutung ist (siehe die Erläuterungen zu Art. 19 Abs. 1 Bst. b E-BÜPF).

Der Zeitraum, während dem die Randdaten gemäss *Absatz 3* rückwirkend angefordert werden können, wird von sechs auf zwölf Monate verlängert. Diese Verlängerung zielt auf eine effektivere Verfolgung von Straftaten ab. Entsprechend wird die Aufbewahrungsdauer der Randdaten verlängert (Art. 19 Abs. 4 und Art. 26 Abs. 5 E-BÜPF). Für weitere Informationen siehe die Erläuterungen zu den Artikeln 19 Absatz 4 und 26 Absatz 5 E-BÜPF.

Art. 274 Abs. 4

Der Wortlaut von *Artikel 274 Absatz 4 Buchstabe a* benötigt eine Anpassung, die sich aus der neuen Fassung von Artikel 271 ergibt.

Die Tatsache, dass ohne Wissen der betroffenen Person in einen nicht öffentlichen Raum eingedrungen wird, um GovWare in das Datenverarbeitungssystem (beispielsweise in einen Computer) einzuführen, das sich in diesem Raum befindet, stellt einen ausserordentlich starken Eingriff dar. Vor diesem Hintergrund ist das Erfordernis einer ausdrücklichen Genehmigung nach *Artikel 274 Absatz 4 Buchstabe b* durchaus gerechtfertigt. In diesem Zusammenhang ist darauf hinzuweisen, dass das Einführen von GovWare in das betreffende Datenverarbeitungssystem in gewissen Fällen je nach Umständen aus der Ferne, beispielsweise per E-Mail, erfolgen kann (siehe auch die Erläuterungen zu Art. 269ter). Damit das Zwangsmassnahmengericht auf diese Ausführungsmodalität aufmerksam gemacht wird, wird der Staatsanwaltschaft die Pflicht nach 269ter Absatz 2 Buchstabe b auferlegt (siehe auch die Erläuterungen zu Art. 269ter Abs. 2 Bst. b).

91 Laurence Aellen/Frédéric Hainard, Secret professionnel et surveillance des télécommunications, Jusletter 23.3.2009, Rz. 21 ff.; Nathalie Zufferey/Jean-Luc Bacher, Commentaire romand: Code de procédure pénale suisse, Basel 2011, Art. 271 StPO N 18.

Art. 278 Abs. 1bis

Der Verweis in *Artikel 278 Absatz 1bis* muss geändert und ergänzt werden. Der Verweis auf Artikel 3 des geltenden BÜPF muss durch den Verweis auf Artikel 35 E-BÜPF ersetzt werden. Es bedarf auch eines Verweises auf Artikel 36 E-BÜPF, da sich dieser Artikel wie Artikel 35 E-BÜPF nicht auf ein laufendes Strafverfahren bezieht (siehe die Erläuterungen zu Art. 36 E-BÜPF) und da Zufallsfunde auch bei einer Ausgangslage möglich sind, auf die sich dieser Artikel bezieht.

Art. 279 Abs. 3 erster Satz

Terminologische Anpassungen, siehe dazu die Erläuterungen zu Artikel 270 Einleitungssatz und Buchstabe b Ziffer 1.

Militärstrafprozess vom 23. März 1979[92]

Art. 70bis (neu) Einsatz von besonderen technischen Geräten zur Überwachung des Fernmeldeverkehrs

Siehe sinngemäss die Erläuterungen zu Artikel 269bis StPO.

Art. 70ter (neu) Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs

Siehe sinngemäss die Erläuterungen zu Artikel 269ter StPO, abgesehen von Absatz 1 Buchstabe b zur Beschränkung auf den Deliktskatalog (und der damit zusammenhängenden Begründung). Entsprechend dem Verweis in Artikel 73*a* Absatz 1 Buchstabe a MStP gilt für verdeckte Ermittlungen grundsätzlich der gleiche Deliktskatalog wie für die Überwachung des Post- und Fernmeldeverkehrs, wobei Artikel 73*a* Absatz 2 MStP – dessen Verweis auf Artikel 286 Absatz 2 StPO aus Gründen der Kohärenz in *Absatz 2bis* übernommen werden muss – vorbehalten bleibt.

Art. 70a Einleitungssatz und Bst. b Ziff. 1

Die Erläuterungen zu Artikel 270, Einleitungssatz und Buchstabe b Ziffer 1 StPO gelten analog auch für *Artikel 70a, Einleitungssatz und Buchstabe b Ziffer 1*.

Art. 70b

Artikel 70b wird genauer formuliert und ergänzt.

Es wird vorgeschlagen, anstelle der Vernehmlassungsversion von *Absatz 1* die gegenwärtige Formulierung beizubehalten und diese zu ergänzen (vgl. unten) ist doch die bestehende Formulierung klar, während aus der Vernehmlassungsversion geschlossen werden könnte, dass selbst jene Daten, die nicht ausgesondert wurden, vom Untersuchungsrichter nicht verwertet werden dürfen. Die Aussonderung der Daten kann unter der Leitung des Präsidenten des Militärgerichts unter Verwendung technischer Massnahmen erfolgen, die es beispielsweise ermöglichen, nur den Verkehr mit ausgewählten Teilnehmerinnen und Teilnehmern bzw. Anschlüssen

92 SR **322.1**

aufzubewahren. Es besteht kein Grund, in der Akte Informationen aufzubewahren, die in keinem Zusammenhang mit den Ermittlungen stehen und dem Berufsgeheimnis unterstehen. *Absatz 1* muss daher ergänzt werden: Wie in Absatz 3 muss vorgesehen werden, dass diese Informationen vernichtet werden müssen und dass sie nicht verwendet werden dürfen.

Die Erläuterungen zu Artikel 271 Absatz 2 StPO gelten analog auch für *Artikel 70b Absatz 2*.

Die Erläuterungen zu Artikel 271 Absatz 3 StPO gelten analog auch für *Artikel 70b Absatz 3*.

Im Weiteren wird der Verweis auf Artikel 75 Buchstaben a und c in *Absatz 3 von Artikel 70b* durch einen Verweis auf Artikel 75 Buchstabe b ersetzt, da diesem Artikel die Artikel 170–173 StPO entsprechen, die in Artikel 271 des erwähnten Gesetzes enthalten sind. Zwischen diesem Artikel und *Artikel 70b* muss eine Parallele vorgesehen werden.

Art. 70c Abs. 2 erster Satz und Abs. 3

Terminologische Anpassungen, siehe dazu die Erläuterungen zu Artikel 70*a*, Einleitungssatz und Buchstabe b Ziffer 1.

Art. 70d Teilnehmeridentifikation, Standortermittlung und technische Merkmale des Verkehrs

Die Erläuterungen zu Artikel 273 Sachüberschrift und Absätze 1 und 3 StPO *gilt* analog auch für *Artikel 70d Sachüberschrift und Absätze 1 und 3*.

Art. 70e Abs. 4

Siehe sinngemäss die Erläuterungen zu Artikel 274 Absatz 4 StPO.

Art. 70k Beschwerde

Terminologische Anpassungen, siehe dazu die Erläuterungen zu Artikel 70*a*, Einleitungssatz und Buchstabe b Ziffer 1.

Fernmeldegesetz vom 30. April 1997[93]

Art. 6a (neu) Sperrung des Zugangs zu Fernmeldediensten

In *Artikel 6a* ist für die Anbieterinnen von Fernmeldediensten ausdrücklich eine Pflicht vorgesehen, den Zugang zur Telefonie und zum Internet unter den erwähnten Bedingungen zu sperren. Damit wird verhindert, dass diese Pflicht auf eine weite Auslegung von Artikel 21 E-BÜPF abgestützt werden muss. Die erwähnte Pflicht hat den Zweck, einen Beitrag zur Identifikation von Personen zu leisten, die ohne Abonnementsverhältnis Zugang zur Telefonie oder zum Internet haben, indem sie beispielsweise Prepaid-SIM-Karten, Prepaid-Wireless-Karten und andere Mittel für den Zugang zum Festnetz verwenden. Die Fernmeldedienstanbieterinnen müssen

93 SR **784.10**

insbesondere auf Grundlage der Informationen der Strafbehörden, namentlich der Strafverfolgungsbehörden, ihrer Pflicht nach Sperrung des Zugangs nachkommen. Es obliegt nicht dem Dienst, das BAKOM oder die Anbieterinnen zu kontaktieren, damit sie die Sperrung vornehmen. Die Strafbehörden melden dem Dienst jedoch die Tatsache, die zur Sperrung geführt hat, damit er überprüfen kann, ob die Anbieterinnen von Fernmeldediensten die Massnahmen, die sie ergreifen müssen, tatsächlich ergriffen haben (siehe Erläuterungen zu Art. 21 E-BÜPF). Ist dies nicht der Fall, so können die Artikel 39–41 E-BÜPF angewendet werden.

Aus Gründen der Praktikabilität ist die oben erwähnte Pflicht zur Sperrung des Zugangs auf die folgenden Situationen beschränkt: Auf Situationen, in denen Kundinnen und Kunden der Fernmeldedienstanbieterinnen bei der Aufnahme und Registrierung der Kundenbeziehung (siehe die Erläuterungen zu Art. 21 E-BÜPF) die Identität einer Person verwendet haben, die nicht existiert oder die der Aufnahme der Kundenbeziehung nicht vorgängig zugestimmt hat, sowie auf Situationen, in denen die betreffenden Kundinnen und Kunden bei der Aufnahme der Kundenbeziehung ein Dokument vorgelegt haben, das nicht den Anforderungen nach Artikel 23 E-BÜPF entspricht, d.h. auf Situationen, bei denen die Kontrolle vor der Aufnahme der betreffenden Kundenbeziehung nicht vorschriftsgemäss durchgeführt wurde (siehe die Erläuterungen zu Art. 23 E-BÜPF). Hingegen ginge es auch unter dem Gesichtspunkt der Beeinträchtigung der persönlichen Freiheit zu weit, wenn nach einer vorschriftsgemässen Überprüfung der Identität verlangt würde, den Zugang zur Telefonie und zum Internet zu sperren, falls die betreffenden Kunden nicht mehr mit den Kundinnen oder Kunden übereinstimmen, die bei der Aufnahme der Kundenbeziehung registriert wurden. Denn ein Mobiltelefon, das mit einer Prepaid-SIM-Karte ausgestattet ist, kann beispielsweise unter absolut normalen Voraussetzungen, d.h. ohne dass dieses Telefon zwangsläufig im Zusammenhang mit einer Straftat verwendet wird, über einen kürzeren oder längeren Zeitraum einem Freund ausgeliehen werden. Im Übrigen würde eine solche Regelung voraussetzen, dass für die Kundinnen und Kunden der Fernmeldedienstanbieterinnen die Pflicht vorgesehen werden müsste, die betreffende Kundenbeziehung zu erneuern. Und für die Anbieterinnen von Fernmeldediensten müsste die Pflicht festgelegt werden, die Kundschaft zu kontrollieren und zu registrieren, die nicht mit den Kundinnen und Kunden übereinstimmt, die bei der Aufnahme der Kundenbeziehung registriert wurde. Dies wäre mit übertriebenen Formalitäten und einem entsprechenden administrativen Aufwand verbunden.

3 Auswirkungen

3.1 Auswirkungen auf den Bund

Gemäss der Kompetenz aus Artikel 38 Absatz 4 E-BÜPF soll der Bundesrat die Höhe der Gebühren festlegen.

Die Kosten, welche dem Dienst im Rahmen der Erfüllung seiner gesetzlichen Aufgaben entstehen, werden durch die Erhebung von Gebühren finanziert. Aufgrund der Tatsache, dass der Dienst seine Aufgaben zurzeit nicht vollständig kostendeckend erbringt (Kostendeckungsgrad 54 Prozent im Jahr 2012), lässt es sich nicht vermeiden, dass dem Bund effektive zusätzliche Kosten anfallen, falls der Bundesrat den Deckungsgrad nicht deutlich anhebt. Es stellt sich die Frage, ob es sachgerecht ist,

am heutigen (tiefen) Kostendeckungsgrad festzuhalten, ist die Strafverfolgung doch eine kantonale Aufgabe.

Der gesamte gesteigerte finanzielle und personelle Ressourcenbedarf muss aber immer vor dem Hintergrund der Verbesserungen im Bereich der Strafverfolgung gesehen werden, die das neue BÜPF bringen wird.

Die finanziellen Auswirkungen des vorliegenden Entwurfes unter dem Gesichtspunkt des Personalbedarfs des Dienstes und dessen Betriebskosten sowie Investitionskosten werden wie folgt veranschlagt:

- Artikel 2 Buchstaben b–f E-BÜPF bedingt eine Unterscheidung verschiedener Anbieterinnen von Fernmeldedienstleistungen mit unterschiedlichen Verpflichtungen und führt zu einer wesentlich höheren Zahl von Verpflichteten. Die Anzahl der derzeit rund 50 aktiven Anbieterinnen wird voraussichtlich auf 150–200 neue Ansprechpartnerinnen des Dienstes anwachsen. Dies wird zu einem wesentlich grösseren Betreuungsaufwand und somit zu einem zusätzlichen Aufwand im Tagesgeschäft und im Pikettdienst des Dienstes führen. Weiter sieht Artikel 5 E-BÜPF vor, dass der Dienst im Konsultativorgan vertreten ist, das das EJPD schaffen kann. Diese Faktoren werden die Schaffung von 1 neuen Vollzeitstelle, zusätzliche Betriebskosten von 300 000 Franken pro Jahr sowie einmalige Investitionskosten von 150 000 Franken (insbesondere für Netzausbauten und Netzanpassungen) notwendig machen.
- Die Artikel 6–14 E-BÜPF führen zu einer personellen Aufstockung um 4 Vollzeitstellen, 2,15 Millionen Franken Betriebskosten pro Jahr und Investitionskosten von 1,6 Millionen Franken. Diese Kosten sind vor allem auf den Betrieb des neuen Informationssystems zur Langzeitspeicherung von Daten aus Überwachungsmassnahmen zurückzuführen. Das System muss unter anderem die sichere und integere Aufbewahrung einer gewaltigen Datenmenge während einer langen Zeitdauer gewährleisten. Hinzu tritt die Gewährleistung allfälliger künftiger Schnittstellen zu den Informationssystemen der Strafverfolgungsbehörden. Die zusätzlichen Kosten berücksichtigen namentlich den Aufwand für Anschaffung neuer Infrastruktur, Abschreibungen alter Systemkomponenten, Netzwerk-, Rechenzentrums- und Lizenzkosten, Support- und Wartungsverträge sowie die Umsetzung der einschlägigen Sicherheitsvorgaben.
- Artikel 15 Absatz 2 E-BÜPF, Artikel 16 E-BÜPF und Artikel 18 E-BÜPF erweitern die Auskunftsleistungen des Dienstes und weisen ihm neue Aufgaben im Bereich Schulung und der technischen Arbeit sowie bei der Qualitätskontrolle zu. Dies bedingt die Schaffung von insgesamt 3 neuen Vollzeitstellen sowie 800 000 Franken Betriebskosten pro Jahr und 600 000 Franken Investitionskosten, um zum einen die notwendige Schulungsumgebung aufbauen und betreiben zu können und zum andern die geforderten Qualitätskontrollen umsetzen zu können.
- Die neuen Aufgaben des Dienstes bei der Überwachung des Fernmeldeverkehrs – insbesondere gemäss Artikel 26 Absatz 2, 32 und 33 E-BÜPF – machen 4 neue Vollzeitstellen, jährliche Betriebskosten von 500 000 Franken und einmalige Investitionskosten von 700 000 Franken notwendig. Die genannten Bestimmungen führen zu einer Verlagerung der Pflichten von gewissen Fernmeldedienstanbieterinnen hin zum Dienst (im Falle von

Anbieterinnen, die von allen oder einem Teil ihrer Pflichten befreit worden sind, aber eine Überwachung durch den Dienst dulden müssen). Dieser wird hierzu entsprechende Überwachungsinfrastrukturen bereitzustellen haben und zunehmend externe Unterstützungsleistungen erbringen, Anpassungen an Informatiksystemen vornehmen sowie Installationen vor Ort bei den betroffenen Fernmeldedienstanbieterinnen machen müssen. Nicht zuletzt entsteht diesbezüglich auch ein erhöhter Schulungs- und Ausbildungsbedarf der Mitarbeiterinnen und Mitarbeiter des Dienstes.

– Die Artikel 40 und 41 E-BÜPF weisen dem Dienst neu aufsichtsrechtliche und verwaltungsstrafrechtliche Kompetenzen zu, deren Wahrnehmung die Schaffung einer neuen Vollzeitstelle bedingt.

Zusammenfassend werden die personellen und finanziellen Auswirkungen des vorliegenden Gesetzesentwurfs wie folgt prognostiziert:

– Die Schaffung von 13 zusätzlichen Vollzeitstellen;
– 3,05 Millionen Franken Investitionskosten;
– eine Erhöhung der jährlichen Betriebskosten um 3,75 Millionen Franken (exklusive Personalkosten).

Es wird darauf hingewiesen, dass die Kostenschätzung nur die Finanzierung der ausgeführten qualitativen Massnahmen berücksichtigt. Eventuelle finanzielle Auswirkungen aufgrund einer quantitativen Zunahme von Überwachungsmassnahmen, welche sich aus der Ausdehnung des Geltungsbereichs theoretisch ebenfalls ergeben könnten, können dagegen im heutigen Zeitpunkt nicht abgeschätzt werden.

3.2 Auswirkungen auf die Kantone

Die künftige Entwicklung der Kosten im Bereich der Überwachung des Post- und Fernmeldeverkehrs wird sich auf die Höhe der Gebühren auswirken.

Der Übergang zum neuen Informatiksystem des Dienstes zur Verarbeitung der Daten aus der Überwachung des Fernmeldeverkehrs dürfte für die Kantone tiefere Ausrüstungskosten zur Folge haben. Die Mehrkosten für den Bund aufgrund der längeren Fristen für die Aufbewahrung der Daten beim Dienst könnten sich hingegen auf die von den Strafverfolgungsbehörden, namentlich der Kantone, zu entrichtenden Gebühren auswirken (siehe die allgemeinen Erläuterungen in Ziff. 2.2). Bezüglich der Gebühren siehe die Erläuterungen zu Artikel 38 E-BÜPF.

3.3 Auswirkungen auf die Wirtschaft

Der vorliegende Entwurf hat für die nach BÜPF mitwirkungspflichtigen Personen zusätzliche Kostenfolgen. Insbesondere was die Anbieterinnen von Fernmeldediensten anbelangt, ist dieser Kostenanstieg indessen zu relativieren: Bei diesen Unternehmen entsprechen die Überwachungskosten nämlich nur einem geringen Betrag im Vergleich zu ihrem Umsatz. Der Kostenanstieg ist auch angesichts des Effizienzgewinns zu relativieren, der dank dem neuen BÜPF bei der Verfolgung von Straftaten erzielt wird. Es gilt zudem darauf hinzuweisen, dass der Bundesrat gemäss Artikel 26 Absatz 6 E-BÜPF Anbieterinnen von Fernmeldediensten von bestimmten

gesetzlichen Pflichten befreien kann – insbesondere wenn sie Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten –, was sich auf die Höhe der zu tragenden Kosten auswirkt.

4 Verhältnis zur Legislaturplanung

Der vorliegende Entwurf ist in der Botschaft vom 25. Januar 2012[94] über die Legislaturplanung 2011–2015 vorgesehen.

5 Rechtliche Aspekte

Das neue BÜPF beruht auf den Artikeln 92 Absatz 1 und 123 Absatz 1 BV, die dem Bund die Zuständigkeit für die Post- und Fernmeldedienste und für die gesetzlichen Bestimmungen im Bereich des Strafrechts und des Strafverfahrens zuweisen.

Es verursacht keine verfassungsrechtlichen Probleme oder Probleme im Zusammenhang mit dem Völkerrecht.

Artikel 13 Absatz 1 BV, Artikel 8 Absatz 1 EMRK und Artikel 17 Absatz 1 des Internationalen Paktes vom 16. Dezember 1966[95] über bürgerliche und politische Rechte garantieren das Post- und Fernmeldegeheimnis, mit anderen Worten: das Recht auf Schutz der Korrespondenz wie auch der Beziehungen, die mittels Post und Fernmeldediensten aufgenommen werden. Dieses Recht ist ein wesentlicher Aspekt des Schutzes der Privatsphäre. Die Überwachung der Korrespondenz und der Beziehungen, die mittels Post und Fernmeldediensten aufgenommen werden, stellen einen schweren Grundrechtseingriff dar. Gemäss Artikel 36 BV und Artikel 8 EMRK muss die Einschränkung eines Grundrechts durch eine gesetzliche Grundlage gedeckt sein, im öffentlichen Interesse liegen und hinsichtlich des angestrebten Ziels verhältnismässig sein. Der Kerngehalt der Grundrechte ist zudem unantastbar. Die Massnahmen zur Überwachung des Post- und Fernmeldeverkehrs müssen deshalb in einem Gesetz im formellen Sinn präzisiert sein. Ein schwerer Eingriff erfordert prinzipiell eine klare und präzise, formell-gesetzliche Grundlage. Die Verständlichkeit des Gesetzes erfordert, dass die Formulierung hinreichend bestimmt ist, damit die Rechtsunterworfenen die Konsequenzen einer bestimmten Handlung voraussehen und sich bei Bedarf von einer Fachperson beraten lassen können[96]. Die gesetzlichen Minimalgarantien im Sinne von Artikel 8 EMRK gegen Machtmissbrauch lauten wie folgt: Die Eignung der Straftat, eine Überwachungsanordnung zu begründen; die Bezeichnung der Personenkategorien, die überwacht werden können; die Befristung für die Durchführung der Massnahme; das Verfahren für die Überprüfung; die Regelung des Gebrauchs und der Aufbewahrung der gesammelten Daten; Vorsichtsmassnahmen für den Schutz der Daten bei der Übermittlung an andere Parteien; Bedingungen, unter denen die Löschung oder Vernichtung der Aufzeich-

94 BBl **2012** 481
95 SR **0.103.2**
96 BGE **123** I 112, E. 7a.

nungen erfolgen kann oder muss[97]. Diese Voraussetzungen sind durch den vorliegenden Gesetzesentwurf erfüllt.

Die Anforderungen des Übereinkommens des Europarates vom 23. November 2001[98] über die Cyberkriminalität sind ebenfalls erfüllt.

Das neue BÜPF enthält Bestimmungen zur Übertragung von Rechtsetzungskompetenzen an den Bundesrat und an die Kantone.

97 Vgl. u.a. die Entscheide des EGMR *Kopp c. Schweiz* vom 25. März 1998, § 64 und 72, Receuil 1998-II und *Liberty u.a.c. Vereinigtes Königreich* vom 1. Oktober 2008, Requête No 58243/00, § 59 ff. (mit weiteren Hinweisen).

98 SR **0.311.43**