



VPB 1/2012 vom 1. Mai 2012

---

2012.3 (S. 28–54)

## Überwachung des Fernmeldeverkehrs: Pflichten der Dienst-anbieterinnen bei Überwachungsmassnahmen im Internet

EJPD, Bundesamt für Justiz

Gutachten vom 16. April 2010

---

**Stichwörter:** Überwachung des Fernmeldeverkehrs/Internetverkehrs bzw. von Internet-Anschlüssen, Wirtschaftsfreiheit, Übertragung öffentlicher Aufgaben auf Private bzw. Beizug Privater bei der Erfüllung öffentlicher Aufgaben, Anbieterinnen von Fernmeldediensten, Internet-(Zugangs-)Anbieterinnen, Dienst Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF), Informatik Service Center EJPD (ISC-EJPD)

**Mots clés:** surveillance de la communication par télécommunication/Internet respectivement des accès Internet, liberté économique, transfert de tâches publiques à des particuliers respectivement recours à des particuliers pour l'accomplissement de tâches publiques, fournisseurs de services de télécommunication, fournisseurs (d'accès à) Internet, Service Surveillance de la correspondance par poste et télécommunication (service ÜPF), Centre de services informatiques DFJP (CSI DFJP)

**Termini chiave:** sorveglianza del traffico delle telecomunicazioni/traffico Internet rispettivamente dell'accesso Internet, libertà economica, trasferimento dei compiti pubblici a privati o ricorso a privati per l'adempimento di compiti pubblici, fornitori di servizi di telecomunicazione, fornitori (di accesso a) Internet, Servizio Sorveglianza della corrispondenza postale e del traffico delle comunicazioni (Servizio SCPT), Centro servizi informatici del Dipartimento federale di giustizia e polizia (CSI DFJP)

---

### Regeste:

1. Aufgrund mangelnder Koordination zwischen dem BÜPF und der VÜPF ist die Rechtslage betreffend die Pflichten der Internet-Anbieterinnen ausserhalb des Katalogs von Artikel 24 VÜPF unsicher. Nach der Einschätzung des BJ sind die Anbieterinnen nur zu den Überwachungen gemäss dem Katalog verpflichtet (Teilfrage a). Daher sind auch nur in diesem Rahmen verpflichtet, sich technisch auf Überwachungen vorzubereiten (b), und sie müssen nur in diesem Rahmen die Kosten dieser technischen Vorbereitung selber tragen (c). Eine weitergehende Verpflichtung zur technischen Aufrüstung kann ohne eine Revision der VÜPF nicht eingeführt werden.

2. Die beim Dienst ÜPF und bei den Internet-Anbieterinnen entstehenden Kosten für in Artikel 24 VÜPF nicht vorgesehene Überwachungen können auf die anordnenden Behörden überwältzt werden. Es ist jedoch zu beachten, dass aufgrund der unsicheren Rechtslage betreffend die materielle Verpflichtung der Anbieterinnen zur technischen Vorbereitung (Frage 1) die Abgrenzung zwischen zu überwältzenden variablen Kosten und nicht zu überwältzenden Fixkosten mit einiger Rechtsunsicherheit behaftet ist.

3. Der Dienst ÜPF kann überprüfen, ob die Fernmeldedienst-Anbieterinnen ihre Pflicht erfüllen, sich technisch auf die in Gesetz und Verordnung vorgesehenen Überwachungen vorzubereiten. Er kann diese Verpflichtung durch Verfügungen konkretisieren, aber nicht ausweiten.

**Regeste:**

1. En raison de l'absence de coordination entre la LSCPT et l'OSCPT, la situation juridique concernant les obligations des fournisseurs Internet est, en dehors du catalogue de l'art. 24 OSCPT, incertaine. Selon l'OFJ, les fournisseurs ne sont tenus de mettre en œuvre que les surveillances prévues dans le catalogue (première partie de la question). Par conséquent, ils ne sont tenus d'entreprendre les préparations techniques en vue des surveillances que dans le cadre du catalogue (deuxième partie de la question), et ils ne doivent supporter les coûts de ces préparations que dans ce cadre-là (troisième partie de la question). L'obligation de procéder à des préparatifs techniques ne peut pas être étendue sans révision de l'OSCPT.

2. Les coûts engendrés auprès du Service ÜPF et des fournisseurs Internet par les surveillances non prévues à l'art. 24 OSCPT, peuvent être répercutés sur les autorités qui les ont ordonnées. On observera cependant que la délimitation entre les coûts variables (à répercuter) et les coûts fixes (à supporter par les fournisseurs) est entachée d'une certaine insécurité juridique liée aux incertitudes (juridiques) concernant l'obligation matérielle des fournisseurs d'entreprendre des préparatifs techniques.

3. Le Service ÜPF est habilité à vérifier si les fournisseurs de services de télécommunication s'acquittent de leur obligation d'entreprendre des préparatifs techniques en vue des surveillances prévues par la loi et l'ordonnance. Il peut concrétiser cette obligation par voie de décisions; il ne peut en revanche pas l'élargir.

**Regesto:**

1. Data la mancanza di coordinamento tra la LSCPT e l'OSCPT, la situazione giuridica concernente gli obblighi dei fornitori Internet al di fuori del catalogo di cui all'articolo 24 OSCPT non è certa. Secondo l'UFG i fornitori sono tenuti a esercitare soltanto le sorveglianze previste nel catalogo (prima parte della questione). Sono pertanto tenuti a prepararsi sul piano tecnico per le sorveglianze soltanto nei limiti del catalogo (seconda parte della questione) e devono sostenere i costi di questi preparativi unicamente in questo quadro (terza parte della questione). Senza una revisione dell'OSCPT, l'obbligo di procedere a preparativi tecnici non può essere esteso.

2. I costi occasionati al Servizio SCPT e ai fornitori Internet per le sorveglianze non previste all'articolo 24 OSCPT possono essere scaricati sulle autorità che le hanno ordinate. Va tuttavia osservato che la delimitazione tra i costi variabili da scaricare e i costi fissi non scaricabili è caratterizzata da una certa insicurezza giuridica dovuta alle incertezze (giuridiche) concernenti l'obbligo materiale dei fornitori di procedere a preparativi tecnici.

3. Il Servizio SCPT è autorizzato a verificare se i fornitori di servizi di telecomunicazione adempiono il loro obbligo di prepararsi sul piano tecnico per le sorveglianze previste dalla legge e dall'ordinanza. Può concretizzare questo obbligo con decisioni; non può invece estenderlo.

**Rechtliche Grundlagen:**

Art. 5 Abs. 1 und 2, 27, 36 und 94 BV; Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1, insb. Art. 15, 16 und 17); Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11, insb. Art. 16, 24, 26 und 33 Abs. 1<sup>bis</sup>); Art. 4 der Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1); Fernmeldegesetz vom 30. April 1997 (FMG, SR 784.10)

**Base légales:**

art. 5, al. 1 et 2, art. 27, 36 et 94 Cst.; Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT, RS 780.1, notamment art. 15, 16 et 17); Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (OSCPT, RS 780.11, notamment art. 16, 24, 26 et 33, al. 1<sup>bis</sup>); art. 4 de l'Ordonnance du 7 avril 2004 sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication (RS 780.115.1); Loi du 30 avril 1997 sur les télécommunications (LTC, SR 784.10)

**Base giuridica:**

art. 5 cpv. 1 e 2, art. 27, 36 e 94 Cost.; legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT, RS 780.1, in particolare art. 15, 16 e 17); ordinanza del 31 ottobre 2001 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT, RS 780.11, in particolare art. 16, 24, 26 e 33 cpv. 1<sup>bis</sup>); art. 4 dell'ordinanza del 7 aprile 2004 sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (RS 780.115.1); legge del 30 aprile 1997 sulle telecomunicazioni (LTC, RS 784.10)

---

## Inhaltsverzeichnis

<b>1</b>	<b>Fragestellung</b> .....	<b>33</b>
<b>2</b>	<b>Frage 1 (a): Verpflichtung der Internet-Anbieterinnen, im konkreten Einzelfall Ausleitungen des IP-Verkehrs an den Dienst durchzuführen</b> .....	<b>34</b>
2.1	Wirtschaftsfreiheit .....	34
2.1.1	Beschränkung der Wirtschaftsfreiheit .....	34
2.1.2	Abweichung vom Grundsatz der Wirtschaftsfreiheit .....	34
2.2	Gesetzliche Grundlage .....	35
2.2.1	Anwendbare Rechtsgrundlagen .....	35
2.2.2	Artikel 15 BÜPF .....	35
2.2.2.1	Wortlaut .....	36
2.2.2.2	Systematik .....	38
2.2.2.3	Entstehungsgeschichte .....	38
2.2.2.4	Sinn und Zweck.....	38
2.2.2.5	Zwischenergebnis .....	39
2.2.3	Artikel 24 VÜPF.....	38
2.2.3.1	Wortlaut.....	39
2.2.3.2	Systematik.....	40
2.2.3.3	Entstehungsgeschichte .....	40
2.2.3.4	Sinn und Zweck.....	41
2.2.3.5	Zwischenergebnis .....	41
2.2.4	Artikel 15 Absatz 6 BÜPF als Grundlage, um das Feld der zulässigen Überwachungstypen zu begrenzen.....	40
2.2.4.1	Das Problem.....	41
2.2.4.2	Wortlaut.....	42
2.2.4.3	Systematik.....	43
2.2.4.4	Entstehungsgeschichte .....	43
2.2.4.5	Sinn und Zweck.....	43
2.2.4.6	Verfassungskonforme Auslegung und Bestimmtheitsgebot im Rahmen des Legalitätsprinzips .....	44
2.2.4.7	Zwischenergebnis .....	45
2.2.5	Artikel 4 der TarifV als Grundlage? .....	44
2.2.6	Zwischenergebnis .....	44
2.3	Öffentliche und private Interessen .....	44
2.4	Verhältnismässigkeit .....	45
2.4.1	Verhältnismässigkeit der Regelung .....	45
2.4.2	Eignung .....	45
2.4.3	Erforderlichkeit .....	45
2.4.4	Interessenabwägung/Zumutbarkeit .....	45
2.4.5	Zwischenergebnis .....	46
2.5	Gleichbehandlung der direkten Konkurrenten .....	46
2.6	Ergebnis/Erfolgschancen .....	46
<b>3</b>	<b>Frage 1 (b): Verpflichtung der Internet-Anbieterinnen, sich technisch auf die Ausleitung des IP-Verkehrs vorzubereiten</b> .....	<b>47</b>
3.1	Grundrechtseingriff .....	47
3.2	Gesetzliche Grundlage .....	47
3.2.1	Verpflichtung direkt gestützt auf die Gesetzgebung .....	47
3.2.2	Verpflichtung durch Verfügungen des Dienstes .....	47
3.2.2.1	Notwendigkeit gesetzlicher Grundlagen .....	48
3.2.2.2	Zulässigkeit von Verfügungen über die Vorbereitungspflicht .....	49

3.2.2.3	Materielle Grundlagen und Umfang der Verpflichtung .....	49
3.2.2.4	Zwischenergebnis zur Verfügungsbefugnis des Dienstes .....	49
3.2.3	Zwischenergebnis zu den gesetzlichen Grundlagen .....	48
3.3	Öffentliche und private Interessen .....	49
3.4	Verhältnismässigkeit .....	49
3.5	Ergebnis .....	50
<b>4</b>	<b>Frage 1 (c): Tragung der Kosten der technischen Vorbereitung durch die Anbieterinnen .....</b>	<b>50</b>
4.1	Artikel 16 BÜPF .....	50
4.2	Innerhalb des Katalogs von Artikel 24 VÜPF .....	50
4.3	Ausserhalb des Katalogs von Artikel 24 VÜPF .....	50
4.4	Ergebnis .....	51
<b>5</b>	<b>Frage 2: Allfällige Überwälzung der Kosten auf die anordnenden Behörden .....</b>	<b>51</b>
<b>6</b>	<b>Frage 3: «Zertifizierung», «Compliance-Prozess» .....</b>	<b>52</b>
<b>7</b>	<b>Exkurs: Beschwerdeberechtigung der Anbieterinnen .....</b>	<b>52</b>
<b>8</b>	<b>Durchsetzung der richtigen Anwendung der Gesetzgebung durch die Bundesbehörden .....</b>	<b>53</b>
<b>9</b>	<b>Empfehlungen für die Gesetzgebung .....</b>	<b>53</b>

## 1 Fragestellung

*Frage 1: «... ob die Regelungen im BÜPF, VÜPF, der Gebührenverordnung sowie den technischen Richtlinien ausreichend sind, um die Internet Service Provider auf ihre Kosten verpflichtet zu können, Technologien (Mediation Devices) anzuschaffen, mit denen sie die Ausleitung des IP-Überwachungsverkehrs garantieren und durchführen können, die Technologien selber zu installieren, die Technologien selber zu konfigurieren, die notwendigen Compliance-Tests durchzuführen und die Ausleitung der Überwachungsdaten bis zum Dienst sicherzustellen.»*

Zur präziseren Analyse der sich stellenden Rechtsprobleme wird die Frage 1 in drei Teilfragen a–c unterteilt:

- a. Verpflichtung der Anbieterinnen zur Weiterleitung des IP-Verkehrs:
- b. Verpflichtung der Anbieterinnen, sich auf Überwachungen technisch vorzubereiten:
- c. Tragung der Kosten der Vorbereitung durch die Anbieterinnen:

*Frage 2: «... ob die Fernmeldedienst-Anbieterinnen dazu verpflichtet sind, sich zur Sicherstellung der gesetzlich vorgesehenen, permanenten Überwachungsbereitschaft gemäss Art. 16 BÜPF, vorgängig auf der Basis der bestehenden technischen Richtlinien für die Lieferung und Ausleitung der geforderten Überwachungsdaten auf eigene Kosten zertifizieren zu lassen.»*

*Frage 3: «... ob im Falle der Einschätzung, dass die Internet Service Provider nicht auf ihre Kosten verpflichtet werden können, Technologien zur Überwachung des IP-Verkehrs anzuschaffen, die beim Internet Service Provider und beim Dienst entstehenden Kosten auf die anordnende Behörde überwälzt werden können.»*

Das Gutachten behandelt das verwaltungsrechtlich geprägte Verhältnis zwischen den Behörden und den Internet-Anbieterinnen. Strafprozessuale Fragen und insbesondere die rechtliche Stellung der Überwachten sind nicht Thema des Gutachtens und werden nur berührt, wenn dies zur Beurteilung der verwaltungsrechtlichen Fragen notwendig ist.

Unter «Ausleitung» des IP-Verkehrs ist vorliegend die Echtzeitüberwachung im Sinn von Artikel 2 Buchstabe c VÜPF zu verstehen, d.h. die direkte Übermittlung der eigentlichen Kommunikationsdaten sowie der für den Datentransport verwendeten Randdaten wie namentlich Adressen<sup>1</sup>. Wir verwenden synonym das Verb «weiterleiten».

Schon an dieser Stelle ist darauf hinzuweisen, dass die Fragestellung insofern differenziert betrachtet werden muss, als die «Ausleitung des IP-Überwachungsverkehrs» technisch ganz unterschiedliche Sachverhalte erfassen kann. Heute werden über das Internet die verschiedensten Kommunikationskanäle angeboten: Internet-Telefonie, E-Mail, Chat-Plattformen, soziale Netzwerke, Dateitransfer usw. Es muss daher stets genau berücksichtigt werden, welche Akteure (bzw. wessen Geräte) welche Arten von Daten wie bearbeiten (speichern, filtern, umformatieren, weiterleiten usw.).

Der in der Fragestellung verwendete Begriff «Internet Service Provider» wird so interpretiert, dass vorliegend ausschliesslich die «Internet-Anbieterinnen» / «fournisseurs d'accès à Internet» / «offerenti internet» im Sinn von Artikel 2 Buchstabe a der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11) gemeint sind. Diese vermitteln ihren Kunden den Zugang zum Internet, was vor allem der französische Wortlaut klar zum Ausdruck bringt. Sie werden teilweise auch mit dem englischen Ausdruck «Access Provider» bezeichnet<sup>2</sup>. Die Verpflichtungen von Anbieterinnen darauf aufbauender Dienste wie etwa der Internet-Telefonie, von elektronischen Postfächern (E-Mail), von Chat-Plattformen und sozialen Netzwerken usw. werden daher nicht untersucht. Diese Anbieter werden allerdings angesprochen, wo es notwendig scheint, um das zugrundegelegte Verständnis der technischen Vorgänge darzustellen. Wo daher im Folgenden ohne

<sup>1</sup> Siehe zum Begriff der Echtzeitüberwachung auch Jürg Schneider, Internet Service Provider im Spannungsfeld zwischen Fernmeldegeheimnis und Mitwirkungspflichten bei der Überwachung des E-Mail-Verkehrs über das Internet, AJP 2/2005, S. 179–192, 188.

<sup>2</sup> Vgl. wiederum die französische Terminologie «fournisseur d'accès à Internet»; siehe auch den Vernehmlassungsbericht über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes betreffend die strafrechtliche Verantwortlichkeit der Provider und die Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze (Netzwerkriminalität) vom Oktober 2004, Übersicht am Anfang (verfügbar auf [www.bj.admin.ch](http://www.bj.admin.ch) > Themen > Kriminalität > Laufende Rechtsetzungsprojekte > Netzwerkriminalität > Vernehmlassungsverfahren).

weitere Präzisierung von «Internet-Anbieterinnen» oder «Anbieterinnen» die Rede ist, sind stets diejenigen gemeint, die den inhalts-indifferenten Internet-Zugang vermitteln.

## 2 Frage 1 (a): Verpflichtung der Internet-Anbieterinnen, im konkreten Einzelfall Ausleitungen des IP-Verkehrs an den Dienst durchzuführen

Zunächst ist zu prüfen, ob die Anbieterinnen in konkreten Überwachungsfällen verpflichtet sind, auf entsprechende Anweisung des Dienstes ÜPF hin (Art. 13 Abs. 1 Bst. b BÜPF) den IP-Verkehr der überwachten Personen an den Dienst weiterzuleiten. Erst danach kann untersucht werden, ob und inwieweit die Internet-Anbieterinnen verpflichtet sind, sich technisch auf solche Überwachungen vorzubereiten (Teilfrage b, siehe Ziffer 3), und ob sie die Kosten selber tragen müssen (Teilfrage c, siehe Ziffer 4).

### 2.1 Wirtschaftsfreiheit

#### 2.1.1 Beschränkung der Wirtschaftsfreiheit

Die Wirtschaftsfreiheit nach Artikel 27 BV schützt unter anderem die freie Ausübung einer privatwirtschaftlichen Erwerbstätigkeit und in deren Rahmen die freie Wahl der Geschäftspartner und der Betätigungsfelder<sup>3</sup>. Diese Freiheit wird durch die einseitig auferlegte Verpflichtung, dem Staat fernmelde-technische Dienstleistungen zu erbringen, eingeschränkt<sup>4</sup>.

Die Rechtsprechung hat bisher offen gelassen, ob sich die Anbieterinnen von Fernmeldediensten angesichts des noch immer weitgehend staatlich regulierten Fernmeldemarktes überhaupt auf die Wirtschaftsfreiheit berufen können<sup>5</sup>. Es ist kein Grund ersichtlich, die Grundrechtsträgerschaft der privaten *Internet*-Anbieterinnen anzuzweifeln. Soweit sie überhaupt vom Fernmeldegesetz vom 30. April 1997 (FMG, SR 784.10) erfasst werden, beschränken sich die sie betreffenden staatlichen Eingriffe im Wesentlichen auf eine Meldepflicht (Art. 4 FMG) und auf verschiedene Regeln zur Verhinderungen von Missbrauch, insbesondere von Marktmacht (Art. 6–12 FMG). Wohl enthält der Katalog der Grundversorgung heute auch einen Internetanschluss, so dass die Swisscom als Grundversorgungskonzessionärin verpflichtet ist, diesen anzubieten<sup>6</sup>. Dies bedeutet jedoch nicht, dass die privaten Anbieterinnen, die teilweise dieselben Leistungen anbieten, nicht von der Wirtschaftsfreiheit profitieren könnten. Immerhin soll das FMG ja gerade einen wirksamen Wettbewerb beim Erbringen von Fernmeldediensten ermöglichen (Art. 1 Abs. 2 Bst. c FMG).

Die Beschränkung der Wirtschaftsfreiheit ist nach Artikel 36 BV nur zulässig, wenn sie auf einer genügenden gesetzlichen Grundlage beruht (2.1.2), der Wahrung öffentlicher Interessen dient (2.3), verhältnismässig ist (2.4) und die Gleichbehandlung der direkten Konkurrenten respektiert (2.5).

Genügende gesetzliche Grundlagen, öffentliche Interessen und die Einhaltung der Verhältnismässigkeit wären auch ohne Eingriff in die Wirtschaftsfreiheit erforderlich (Art. 5 Abs. 1 und 2 BV).

#### 2.1.2 Abweichung vom Grundsatz der Wirtschaftsfreiheit

Nach Artikel 94 Absätze 1 und 4 BV darf der Bund vom Grundsatz der Wirtschaftsfreiheit nur abweichen, wenn er dafür über eine Grundlage in der Bundesverfassung verfügt. Eine Abweichung vom Grundsatz kann insbesondere darin bestehen, dass Massnahmen ergriffen werden, die sich gegen den Wettbewerb richten<sup>7</sup>. Die Bekämpfung schwerer Straftaten (Art. 3 Abs. 2 BÜPF) und die Suche nach vermissten Personen (Art. 3a BÜPF) bezwecken nicht die Ausschaltung oder Beeinflussung des Wettbewerbs, sondern dienen polizeilich geprägten öffentlichen Interessen. Daher ist eine Abweichung vom Grundsatz der Wirtschaftsfreiheit nicht ersichtlich.

<sup>3</sup> Siehe etwa Klaus A. Vallender, St. Galler Kommentar zu Art. 27 BV, 2. Auflage 2008, Rz. 20.

<sup>4</sup> Entscheid des Bundesverwaltungsgerichts A-2335/2008 vom 10. März 2009, E. 9.1.

<sup>5</sup> Bundesverwaltungsgericht a.a.O., im Anschluss an BGE 131 II 13 E. 6.4.1.

<sup>6</sup> Art. 16 FMG i.V.m. Art. 15 ff., insb. Art. 16 Abs. 2 Bst. c der Verordnung vom 9. März 2007 über Fernmeldedienste, FDV, SR 784.101.1.

<sup>7</sup> Art. 94 Abs. 4 BV; vgl. Klaus A. Vallender, St. Galler Kommentar zu Art. 94 BV, Rz. 5–6.

## 2.2 Gesetzliche Grundlage

### 2.2.1 Anwendbare Rechtsgrundlagen

Auf die Überwachung des Internet-Verkehrs sind namentlich anwendbar:

- das Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (*BÜPF*, SR 780.1);
- die Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (*VÜPF*, SR 780.11);
- die Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (im Folgenden *TarifV*, SR 780.115.1);
- im Hintergrund das Fernmeldegesetz vom 30. April 1997 (*FMG*, SR 784.10) und seine Ausführungsbestimmungen.

Dazu kommen die *technischen und administrativen Richtlinien* des Dienstes ÜPF nach Artikel 33 Absatz 1<sup>bis</sup> VÜPF<sup>8</sup>. Diese nicht veröffentlichten Richtlinien können nicht als gesetzliche Grundlage dienen, da ihnen der Rechtssatzcharakter abgeht. Sie werden nicht als Rechtssätze, sondern eben als Richtlinien bezeichnet, nicht in die Landessprachen übersetzt und nicht in der Amtlichen Sammlung des Bundesrechts publiziert und können somit nicht die Rechtswirkungen von Rechtssätzen entfalten<sup>9</sup>.

Der Erlass von Rechtssätzen durch eine Behörde unterhalb der Departementsstufe wäre ohne Grundlage im Gesetz selber ohnehin unzulässig<sup>10</sup>, und das BÜPF enthält keine entsprechende Klausel. Das Bundesverwaltungsgericht führte in einem obiter dictum aus, der Bundesrat könne sich auf Artikel 62 FMG stützen, um dem Dienst ÜPF Rechtssetzungskompetenzen im Bereich des BÜPF zu übertragen<sup>11</sup>. Dies erscheint insofern unzutreffend, als das «Bundesamt» im Sinn des FMG ausschliesslich das BAKOM ist (Art. 4 Abs. 1 FMG) und nicht etwa auch der Dienst. Zudem regelt Artikel 62 FMG nur den Vollzug «dieses» Gesetzes (Abs. 1) und nicht etwa auch denjenigen des BÜPF. Artikel 62 FMG könnte daher nicht als Grundlage für eine Gesetzgebungs-Subdelegation an den Dienst dienen. Schliesslich ist noch einmal darauf hinzuweisen, dass der Bundesrat dem Dienst nur den Auftrag erteilt hat, *Richtlinien* zu erlassen, nicht Rechtssätze (Art. 33 Abs. 1<sup>bis</sup> VÜPF).

Die Richtlinien können somit keine gesetzliche Grundlage abgeben, sondern nur die Praxis der Behörde erklären oder – sofern sie nicht im Einzelfall durch eine Verfügung umgesetzt werden – mit interner Wirkung zu einer Vereinheitlichung der Praxis beitragen<sup>12</sup>.

### 2.2.2 Artikel 15 BÜPF

#### 2.2.2.1 Wortlaut

Artikel 15 Absatz 1 BÜPF ist die zentrale Vorschrift zu den Pflichten der Anbieterinnen im Rahmen der Überwachung des Fernmeldeverkehrs:

«Die Anbieterinnen von Fernmeldediensten sind verpflichtet, dem Dienst auf Verlangen *den Fernmeldeverkehr* der überwachten Person sowie die Teilnehmeridentifikation und Verkehrs- und Rechnungsdaten zuzuleiten ...»

«... transmettre *les communications* de la personne surveillée ainsi que les données permettant d'identifier les usagers et celles relatives au trafic et à la facturation ...»

<sup>8</sup> Siehe z.B. Lawful Interception of telecommunications traffic – Technical Guideline for the implementation of lawful measures for monitoring telecommunications / TR TS, limited to Annex G, vom 1. August 2009, Ziffern 5 und 6 zu den Anforderungen an die Weiterleitung der Überwachungsdaten.

<sup>9</sup> Vgl. Art. 8 Abs. 1 des Publikationsgesetzes vom 18. Juni 2004, SR 170.512.

<sup>10</sup> Art. 48 Abs. 2 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997, RVOG, SR 172.010.

<sup>11</sup> Bundesverwaltungsgericht, Entscheid A-2045/2006 vom 17. Februar 2009, E. 3.2.2.

<sup>12</sup> Vgl. zum Ganzen den Gesetzgebungsfaden des Bundesamtes für Justiz, 3. Auflage Bern 2007, Gliederungsziffer 572; Pierre Tschannen / Ulrich Zimmerli / Markus Müller, Allgemeines Verwaltungsrecht, 3. Auflage Bern 2009, § 15–16; Kopfschaltungs-Entscheid des Bundesverwaltungsgerichts, A-2335/2008 vom 10. März 2009, E. 7.4.

«... trasmettere il traffico delle telecomunicazioni della persona sorvegliata, come pure i dati d'identificazione degli utenti e quelli relativi al traffico e alla fatturazione ...»

(Hervorhebungen hinzugefügt)

Aufgrund dieser Formulierung ist klar, dass die Weiterleitungspflicht den *Fernmeldeverkehr* (siehe dazu Art. 3 Bst. b und c FMG) der überwachten Personen betrifft. Allerdings muss die Frage gestellt werden, was im Einzelnen *Gegenstand der Weiterleitungspflicht* der Anbieterinnen ist<sup>13</sup>:

- Ungeachtet des einfachen bestimmten Artikels «der» ist offensichtlich nicht *jeglicher* Fernmeldeverkehr gemeint, der irgendwo im Land oder gar im Ausland mit oder ohne Beteiligung der betreffenden Anbieterin stattfindet. Es versteht sich von selbst, dass die Anbieterinnen nur Daten weiterleiten können, über die sie verfügen.
- Eine Verpflichtung der Zugangs-Anbieterinnen, *jegliche* Art konkreter Kommunikationsvorgänge aus dem Datenstrom ihrer Kunden zu filtern und aufbereitet weiterzuleiten, kann ebenfalls nicht gemeint sein, denn damit würde in vielen Fällen technisch Unmögliches verlangt. So ist es der Zugangs-Anbieterin beispielsweise unmöglich, Daten zu entschlüsseln, die vom Computer eines Benützers verschlüsselt werden und von dort zu demjenigen seines Kommunikationspartners geleitet werden. Diese Situation trifft man beispielsweise bei sogenannten «peer to peer»-Anwendungen («p2p») wie z.B. bei Telefonanrufen von Computer zu Computer mit der Software Skype<sup>14</sup>. So verpflichtet Artikel 15 Absatz 4 zweiter Satz BÜPF die Anbieterinnen denn auch nur dazu, diejenigen Verschlüsselungen zu entfernen, die sie selber angebracht haben<sup>15</sup>.
- Die weitestmögliche Auslegung würde daher *im Rahmen des technisch Möglichen die einzelnen Kommunikationsvorgänge* erfassen. Die Zugangs-Anbieterinnen müssten gestützt auf diese Auslegung verschiedenste Inhalte aus dem Datenstrom ihrer Kunden herausfiltern und aufbereiten, z.B. Gespräche über die IP-Telefonie, mit den verschiedensten Techniken übermittelte Dateien, abgerufene Internetseiten, in Echtzeit über Chat-Protokolle übermittelte Textmitteilungen, in Echtzeit übermittelte Videosequenzen bei der Videotelefonie usw.

Diese weite Interpretation wäre sehr im Interesse der Behörden, da grosse Teile des technischen Gesamtaufwands bei den Anbieterinnen anfallen würde. Für die betroffenen Anbieterinnen könnte dies hingegen sehr unangenehm sein, weil sie sich in vielen Konstellationen auf eine Teildienstleistung beschränken, die ihnen keine echte Herrschaft über die für die Überwachung nötigen (Teil-) Daten vermitteln. Um den Zugang zum Internet zu vermitteln, benötigen die Zugangs-Anbieterinnen keine technischen Einrichtungen, die ein Filtern und Aufbereiten der übertragenen Daten erlauben: Sie müssen bloss Datenpakete an die angegebene Adresse weiterleiten, ohne sich um deren Inhalt zu kümmern.

- Man könnte daher auch auf diejenigen (Teil-) Dienste abstellen, welche die betreffenden Anbieterinnen im technischen Courant normal zu erbringen pflegen. Die Anbieterinnen müssten somit für die Behörden nicht komplexere Dienstleistungen erbringen, als jene, die sie freiwillig ihren Kunden anbieten. Für die reinen Zugangs-Anbieterinnen würde das bedeuten, dass sie den Behörden Datenpakete weiterleiten müssten, die sie nach relativ einfachen Kriterien (insb. nach der IP-Adresse des Empfängers oder der Absenderin) ermitteln müssten. Filtern oder aufbereiten müsste sie die Daten nicht weiter.

Für die Behörden wäre diese Interpretation deutlich weniger interessant, da sie, wenn sie bei den leichter fassbaren Zugangs-Anbieterinnen ansetzen wollen, selber die aufwändige Filterungs- und Umwandlungsarbeit übernehmen oder Dritte damit beauftragen müssten<sup>16</sup>. Die bereits aufbereiteten Kommunikationsinhalte wären nur bei den entsprechenden Anbieterinnen erhältlich. Ob diese aber dem BÜPF überhaupt unterstellt sind, ist fraglich. Zudem können sie sich im Ausland befinden, wodurch sie dem BÜPF sicher nicht unterstehen. Schliesslich benötigen sogenannte Peer-to-Peer-Anwendungen neben den Zugangs-Anbieterinnen gar keine weiteren, dienst-spezifischen Anbieterinnen.

<sup>13</sup> Vgl. für einige technische Aspekte Jean Treccani, *Interceptions électroniques*, in: Ursula Cassani u.a. (Hrsg.), *Mehr Sicherheit – weniger Freiheit*, Chur/Zürich 2003, S. 217–238, S. 227–229.

<sup>14</sup> Vgl. Thomas Hansjakob, *Kommentar BÜPF/VÜPF*, 2. Auflage St. Gallen 2006, Ziffer 3.6.3, S. 60–64.

<sup>15</sup> Vgl. Botschaft BBI 1998 IV 4241, 4281–82.

<sup>16</sup> Zum grossen Aufwand Hansjakob, *Kommentar BÜPF/VÜPF*, 2. Auflage St. Gallen 2006, Einige technische Grundlagen, S. 59.

Es stehen somit die zwei zuletzt genannten Auslegungsmöglichkeiten im Vordergrund. Der Wortlaut von Artikel 15 Absatz 1 BÜPF spricht nicht eindeutig für die engere oder die weitere Interpretation. Der zweite Satz von Absatz 2 desselben Artikels erlaubt jedoch einen Rückschluss auf die Bedeutung von Absatz 1:

«... Alle beteiligten Anbieterinnen sind verpflichtet, *ihre* Daten der beauftragten Anbieterin zu liefern. ...»

«... Tous les fournisseurs de service concernés sont tenus de fournir les données *en leur possession* au fournisseur de service chargé de la surveillance. ...»

«... Tutti gli offerenti interessati sono tenuti a fornire all'offerente incaricato della sorveglianza i dati *di cui dispongono*. ...»

(Hervorhebungen hinzugefügt)

Die Formulierung «ihre Daten» deutet auf die engere Auslegungsvariante hin, da jede Anbieterin primär nur die technische Herrschaft (eine Art «Besitz» im Sinn des Possessivpronomens «ihre») über die von ihr angebotenen konkreten Dienste hat, d.h. die reine Zugangs-Anbieterin über die inhaltsindifferenten Datenpakete; die IP-Telefon-Anbieterin über die Telefonverbindungen, die über ihre Server laufen; der Chat-Plattform-Betreiber über die ausgetauschten Sofortnachrichten, abgerufene Benutzerprofile usw.

Die allgemeinen, nicht auf die Pflichten der Anbieterinnen bezogenen Bestimmungen des Gesetzes geben keine zusätzlichen Hinweise, wie die Weiterleitungspflicht der Anbieterinnen im Internet-Bereich zu verstehen ist. Weder die strafprozessual zentralen Vorschriften von Artikel 3 BÜPF noch die Bestimmungen über die «besonderen Formen der Überwachung» nach Artikel 4 BÜPF zeigen auf, was unter dem Fernmeldeverkehr einer Person im Internet zu verstehen ist. Aus den Artikeln 3a und 5 BÜPF geht zwar hervor, dass das Gesetz drei Hauptkategorien von Informationen unterscheidet, nämlich den Fernmeldeverkehr selber, die Teilnehmeridentifikation und die Verkehrs- und Rechnungsdaten. Auch dies klärt jedoch nicht die Frage, wie der Begriff des Fernmeldeverkehrs hinsichtlich Internet zu handhaben ist.

### 2.2.2.2 Systematik

Die systematische Eingliederung von Artikel 15 und 16 BÜPF bestätigt deren allgemeine Bedeutung für alle Arten von Fernmeldediensten, spricht jedoch im Bereich der Internet-Überwachung nicht gegen die engere Interpretation.

### 2.2.2.3 Entstehungsgeschichte

Der Botschaft zum BÜPF<sup>17</sup> kann keine eindeutige Aussage zur Frage entnommen werden, welche Anbieterinnen im Internetbereich welche Dienstleistungen zuhanden des Staates erbringen müssen. Auf den Seiten 4255–56 wird bloss klargestellt, dass die Internetprovider erfasst sein sollen und dass «die Herausgabe sowohl des Datenverkehrs als auch der beim Provider gespeicherten Randdaten verlangt werden» kann.

Das BÜPF stammt aus einer Zeit, als zumindest in den meisten Köpfen bei der Überwachung des Fernmeldeverkehrs noch relativ klar war, was überwacht wurde: Telefongespräche, Faxedokumente, Telexnachrichten usw. Das Internet war noch eine neue, zwar boomende, aber in den Details nur wenig bekannte Erscheinung. Der Bundesrat ging denn in der Botschaft auch nicht weiter, als dass er sich die Frage stellte, ob das Internet überhaupt erfasst sein sollte. Im Zeitalter des universellen Einsatzes des Internets und der Konvergenz der Medien ist die Sachlage jedoch sehr kompliziert geworden. Die meisten älteren Kommunikationsmittel können in der einen oder anderen Form auch über das Internet angeboten werden.

Im Lauf der parlamentarischen Beratungen wurde Artikel 15 (im Entwurf Art. 13) Absatz 1 BÜPF nicht thematisiert. Diskutiert wurde im Zusammenhang mit diesem Artikel nur der heutige Absatz 2 zur Aufgabenteilung zwischen mehreren Fernmeldedienst-Anbieterinnen und die damals in der Einigungs-

<sup>17</sup> BBI 1998 IV 4241, 4279.

konferenz abgelehnte, 2003 aber als Absatz 5<sup>bis</sup> nachträglich eingeführte Registrierungspflicht für Mobiltelefone ohne Abonnement.<sup>18</sup>

Die Entstehungsgeschichte erlaubt somit keine Aussagen darüber, welche der Auslegungsvarianten vorzuziehen sei.

#### 2.2.2.4 Sinn und Zweck

Einerseits will das BÜPF sicherstellen, dass möglichst jeglicher Fernmeldeverkehr überwacht werden kann: Der Staat möchte seinen Strafverfolgungsbehörden gleich lange Spiesse verschaffen, wie Kriminelle sie mit grosser Selbstverständlichkeit einsetzen. Dies spricht für eine möglichst weite Auslegung der Pflichten der Anbieterinnen.

Andererseits ist es dem Gesetzgeber bekanntlich ein Anliegen, die Wirtschaftsfreiheit im Fernmeldebereich möglichst wenig zu beeinträchtigen (vgl. Art. 1 Abs. 2 Bst. c FMG). Vor diesem Hintergrund ist es auch Aufgabe des BÜPF, für die Gleichbehandlung der Anbieterinnen sowie für einen Interessenausgleich zwischen der Strafverfolgung und den Fernmeldedienst-Anbieterinnen zu sorgen. Dies spricht eher für eine Begrenzung der Pflichten der Anbieterinnen, die durchaus auf der Linie der oben dargestellten engeren Interpretation liegen könnte. Plausibel ist diese Betrachtung insbesondere aus dem Grund, dass die Schaffung gleich langer Spiesse für die Strafverfolgungsbehörden durch die engere Interpretation nicht verunmöglicht wird; bloss der technische Aufwand wird eher dem Staat zugewiesen.

Die teleologische Auslegung tendiert damit eher zur engeren Auslegung, ohne jedoch ein deutliches Resultat zu ergeben.

#### 2.2.2.5 Zwischenergebnis

Das BJ betrachtet die einschränkende Interpretation angesichts des Wortlauts und der teleologischen Auslegung als die plausible. Demzufolge bietet das BÜPF nur (aber immerhin) die Grundlage dafür, die Internet-Anbieterinnen zu Dienstleistungen zu verpflichten, deren technische Komplexität und Aufwandsträchtigkeit sich grob an dem orientieren, was die Anbieterinnen ihren Kunden privatautonom anbieten.

Anzumerken ist hier, dass der Bestimmtheitsgrad des Gesetzes tief ist. Die obenstehenden Ausführungen zeigen deutlich, dass es schwierig ist, alleine aufgrund des sehr knappen Gesetzestextes und der mageren Materialien klare Aussagen über die Pflichten der Anbieterinnen zu machen. Angesichts der hohen technischen Komplexität und der grossen Vielfalt der sich stellenden Aufgaben wäre es zumindest naheliegend, die Pflichten der Anbieterinnen auf Verordnungsstufe präziser zu regeln.

### 2.2.3 Artikel 24 VÜPF

#### 2.2.3.1 Wortlaut

Artikel 24 VÜPF enthält bezüglich der Überwachung der Internet-Zugänge eine Liste von Überwachungstypen. Die Aufzählung wird mit einem Einleitungssatz eingeleitet, der alle nicht genannten Überwachungstypen ausschliesst:

«Folgende Überwachungstypen können angeordnet werden: (...)»

«Les types de surveillance suivants peuvent être ordonnés: (...)»

«Possono essere ordinate le forme di sorveglianza seguenti: (...)»

Der darauf folgende, technisch präzise gefasste Katalog befasst sich ausschliesslich mit dem E-Mail-Verkehr (Bst. a–e und h) und mit den Verkehrs- und Rechnungsdaten bei der dynamischen Zuteilung von IP-Adressen (Bst. f) sowie beim Zugang über ein öffentliches Telefonnetz (Bst. g).

<sup>18</sup> Amtliches Bulletin Nationalrat, AB N 1999 2602, 2613; Amtliches Bulletin Ständerat, AB S 2000 400, 406; AB N 2000 N 866, 869; AB S 2000 560, 561; AB N 2000 1021, 1022; AB S 2000 660.

Die Weiterleitung des gesamten IP-Verkehrs eines Benützers oder einer IP-Adresse ist in der Liste nicht enthalten. Die Verpflichtung der Anbieterinnen zu dieser Weiterleitung entspräche der oben dargestellten engeren Auslegung von Artikel 15 Absatz 1 BÜPF.

Die Weiterleitung von herausgefilterten oder aufbereiteten, nicht das E-Mail betreffenden Bestandteilen des IP-Verkehrs (IP-Telefonie-Verbindungen, Chat-Nachrichten usw.) wird auch nicht genannt. Solche Überwachungen würden von der weiteren Auslegung des Gesetzes gedeckt.

Die Regelung der Verordnung ist daher zumindest nach dem Wortlaut viel enger als Artikel 15 Absatz 1 BÜPF – auch wenn man dessen engerer Interpretation folgt.

### 2.2.3.2 Systematik

Aus den Abschnittsüberschriften ergibt sich, dass neben den Querschnittsbestimmungen (1., 2., 8. und 9. Abschnitt) nur der 6. Abschnitt der Verordnung auf Internet-Überwachungen anwendbar sein kann, nicht etwa auch die Abschnitte 3–5. Insbesondere Artikel 16, der in seinem Buchstaben a eine weit gefasste Grundlage für die Weiterleitung des gesamten Fernmeldeverkehrs mit Ausnahme von Internet enthält, ist auf den Internet-Bereich somit nicht anwendbar. Dass die Verordnung für die Fernmeldeüberwachung mit Ausnahme von Internet die Weiterleitung des gesamten Fernmeldeverkehrs eines Benützers ausdrücklich und prominent anführt, legt den Umkehrschluss nahe, dass diese Option im Internet-Bereich, wo sie nicht genannt ist, nicht gegeben sein soll.

Die Systematik der Verordnung folgt in den drei Bereichen «Postverkehr», «Fernmeldeverkehr mit Ausnahme von Internet» und «Internet» einem klaren Schema (Überwachungsanordnung, Überwachungstypen, Durchführung der Überwachung, Pflichten der Anbieterinnen). Die Überwachungstypen werden zumindest auf Wortlautebene überall abschliessend aufgezählt. Diese Schematreue spricht dafür, dass auch Artikel 24 die zulässigen Überwachungstypen abschliessend aufzählt.

Aus systematischer Perspektive spricht somit alles dafür, dass die Aufzählung abschliessend ist und nur die aufgeführten Überwachungstypen möglich sein sollen.

Da nicht immer klar ist, ob Angebote im Telefonbereich unter Artikel 16 oder Artikel 24 VÜPF fallen<sup>19</sup>, kann hier unter Umständen für die Überwachung von IP-Telefon-Verbindungen unter Berufung auf Artikel 16 VÜPF trotz des IP-Bezugs eine Ausweitung erreicht werden. Anderer Internet-Verkehr kann jedoch nicht mit dem Argument, er werde ja über Telefoninfrastruktur geführt, auch unter Artikel 16 gefasst werden, da die Systematik den Internet-Bereich hier eindeutig ausnimmt.

Abgesehen von diesem telefonspezifischen Abgrenzungsproblem spricht die Systematik deutlich dafür, dass im Internet nur die in Artikel 24 VÜPF genannten Überwachungstypen zulässig sind.

### 2.2.3.3 Entstehungsgeschichte

Aus dem (nicht öffentlichen) Antrag des EJPD und des UVEK an den Bundesrat vom 8. Oktober 2001 zur VÜPF ergibt sich, dass die antragstellenden Departemente der klaren Ansicht waren, Internet-Überwachungen ausserhalb des Katalogs von Artikel 24 VÜPF sollten nicht zulässig sein. Die Einleitung zum 6. Abschnitt der dem Antrag beiliegenden Erläuterungen lautet:

«6. Abschnitt      Überwachung der Internet-Zugänge

Im Interesse einer besseren Übersichtlichkeit wird den Bestimmungen über das Internet ein eigener Abschnitt gewidmet. Dies führt zu gewissen Wiederholungen. Eine andere, weniger leserfreundliche Möglichkeit wäre gewesen, nur noch Bestimmungen aufzunehmen, die von den allgemeinen Bestimmungen über die Überwachung des Fernmeldeverkehrs abweichen. *Vorerst wird die Überwachung der Internet-Anschlüsse auf die E-Mails und auf die Verbindungen über ein öffentliches Telefonienetz beschränkt.*»

(Hervorhebung hinzugefügt)

<sup>19</sup> Es gibt Telefonie-Angebote, bei denen der Benutzer ein «normales» Telefon-Endgerät verwendet (oder eines, das sich zumindest aus seiner Sicht in nichts von einem «normalen» Telefon unterscheidet), und doch laufen die Gespräche ganz oder teilweise über Internet-Verbindungen und das Internet-Protokoll. Zudem verwenden auch die traditionellen Telefon-Anbieterinnen unseres Wissens zumindest für die Langstrecken-Übermittlung teilweise ebenfalls Internet-Verbindungen.

Weshalb hier die dritte Kategorie, nämlich die Verkehrs- und Rechnungsdaten bei der dynamischen Vergabe von IP-Adressen (Art. 24 Bst. f VÜPF), nicht genannt wird, ist unklar. Es handelt sich möglicherweise um ein Versehen. Vielleicht dachte man nicht daran, dass IP-Adressen auch auf anderen Netzen als auf Telefonnetzen dynamisch vergeben werden können (z.B. in Fernseh-Kabelnetzen). Jedenfalls ist die Frage vorliegend kaum entscheidend.

Der (ebenfalls nicht veröffentlichte) Entwurf aus dem Ämterkonsultationsverfahren<sup>20</sup> vom 1. Juni 2001 hatte in seinem Artikel 26 (entspricht dem heutigen Artikel 24) noch eine viel umfangreichere Liste möglicher Überwachungsformen enthalten. Diese nannte insbesondere die Aufzeichnung und Direkt-schaltung der «eingehenden und ausgehenden IP-Datagramme [Datenpakete] zu oder von einer IP-Adresse oder eines Anschlusses einer Teilnehmerin bzw. eines Teilnehmers (einschliesslich deren Inhalt)»<sup>21</sup>. Diese Formulierung hätte für die Weiterleitung des IP-Verkehrs genau der Weiterleitung im Sinn der oben dargestellten engeren Auslegung von Artikel 15 Absatz 1 BÜPF entsprochen und wäre das Pendant zu Artikel 16 Buchstabe a VÜPF gewesen. Sie wurde jedoch aufgrund eines bewussten Entscheids für die definitive Version der Verordnung gestrichen.

Die Entstehungsgeschichte führt also zu einem eindeutigen Ergebnis: Die antragstellenden Departemente gingen davon aus, dass die VÜPF *keine* Internet-Überwachungen ausserhalb des Katalogs von Artikel 24 VÜPF erlauben würde. Somit versteht sich auch von selbst, dass nach dem Willen des Verordnungsgebers keine Pflicht der Anbieterinnen bestehen konnte, weitergehende Überwachungen zu ermöglichen oder durchzuführen. Eine VÜPF-Revision, die den Katalog ausgeweitet hätte, wurde zwar damals bereits angedacht («Vorerst wird ... beschränkt»), bis heute aber nicht vorgenommen.

### 2.2.3.4 Sinn und Zweck

Sinn und Zweck der Regelung erlauben keine eindeutigen Aussagen; es kann im Wesentlichen auf die entsprechenden Ausführungen zum Gesetz (Ziffer 2.2.2.4) verwiesen werden.

### 2.2.3.5 Zwischenergebnis

Wortlaut, Systematik und Entstehungsgeschichte von Artikel 24 VÜPF führen zum gleichen Ergebnis: Die Aufzählung ist abschliessend. Die Bestimmung schliesst – aus sich selbst heraus ausgelegt – die nicht genannten Überwachungstypen im Internet aus. Für die These, wonach die abschliessend formulierte Aufzählung eigentlich nur beispielhaft gemeint sei, findet sich in der Verordnung und in den Materialien dazu kein Hinweis.

Es ist anzumerken, dass dieses Resultat offenbar der gängigen Praxis widerspricht, wonach sehr wohl der gesamte Datenverkehrs bestimmter IP-Adressen oder bestimmte herausgefilterte Kommunikationsvorgänge überwacht werden<sup>22</sup>. Gerichtsentscheide zur Frage, ob diese Praxis legal ist, liegen uns nicht vor. Im Kopfschaltungs-Entscheid des Bundesverwaltungsgerichts ging es um den Telefonverkehr, der von Artikel 16 Buchstabe a VÜPF abgedeckt ist<sup>23</sup>. In den Entscheiden der REKO INUM und des Bundesgerichts betreffend einen Sonderfall einer Internet-Überwachung (Mietleitung/E-Mail) war nur die Entschädigungsfrage Prozessgegenstand<sup>24</sup>.

## 2.2.4 Artikel 15 Absatz 6 BÜPF als Grundlage, um das Feld der zulässigen Überwachungstypen zu begrenzen

### 2.2.4.1 Das Problem

Artikel 15 Absatz 1 BÜPF erfasst den gesamten Fernmeldeverkehr der überwachten Personen. Der Auslegungsspielraum, den diese Vorschrift bietet, betrifft in erster Linie die Frage, welche Anbieterinnen zur Weiterleitung, Filterung und Aufbereitung welcher Daten verpflichtet werden können. Anzei-

<sup>20</sup> Art. 4 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998, RVOV, SR 172.010.1.

<sup>21</sup> Art. 26 Abs. 1 Bst. a Ziff. 3 und Bst. b Ziff. 3 des Ämterkonsultations-Entwurfs; eckige Klammer ergänzt.

<sup>22</sup> Entsprechende telefonische Erklärungen Ihres Mitarbeiters Patrick Schöpf.

<sup>23</sup> Bundesverwaltungsgericht, Entscheid A-2335/2008 vom 10. März 2009.

<sup>24</sup> REKO INUM, Entscheid J-2005-268 vom 25. Oktober 2006; Bundesgericht, Entscheid 1A.255/2006 vom 20. März 2007.

chen, dass nicht der gesamte Fernmeldeverkehr unabhängig vom konkreten technischen Kommunikationskanal erfasst wäre, finden sich nicht.

Artikel 24 VÜPF erlaubt dagegen mit grosser Deutlichkeit ausschliesslich die dort aufgezählten Überwachungstypen, die nur einen kleinen Ausschnitt aus den möglichen Weiterleitungen des Internet-Verkehrs abdecken. Insbesondere die pauschale Weiterleitung des gesamten Verkehrs einer IP-Adresse erlaubt die Verordnung nicht.

Im Folgenden ist daher zu prüfen, ob diese Einschränkung gegenüber Artikel 15 Absatz 1 BÜPF gültig ist.

Es kommt vor, dass Verordnungen des Bundesrats den an sich weiten Geltungsbereich gesetzlicher Vorschriften einschränken. So schränkt etwa Artikel 7 Absatz 1 der Verordnung 1 vom 10. Mai 2000 zum Arbeitsgesetz (ArGV 1, SR 822.111) den Geltungsbereich des Arbeitsgesetzes vom 13. März 1964 (ArG, SR 822.11) ein. Dazu kann sich der Bundesrat jedoch auf eine ausdrückliche Ermächtigung im Gesetz selber berufen (Art. 2 Abs. 2 ArG).

Eine solche Ermächtigung (Delegationsnorm) ist auch im Fall des BÜPF und der VÜPF nötig, da der Unterschied zwischen den beiden fraglichen Bestimmungen wichtige Fragen im Sinn von Artikel 164 Absatz 1 Buchstaben b, c und e BV beschlägt. Die Entscheidung, ob die Strafbehörden nur den E-Mail-Verkehr und verschiedene Kommunikationsranddaten überwachen dürfen oder ob sie Zugriff auf den gesamten Internet-Verkehr haben sollen, ist praktisch von eminenter Bedeutung. Sie hat gewichtige Auswirkungen auf die Strafverfolgung, das Fernmeldegeheimnis, den Schutz der persönlichen Daten der Überwachten und auf die Pflichten der Anbieterinnen.

Wichtige rechtsetzende Bestimmungen in diesem Sinn kann der Bundesrat nur gestützt auf eine Delegationsnorm im Gesetz selber erlassen. Seine allgemeine Kompetenz, Ausführungsvorschriften zu erlassen (Art. 182 Abs. 2 BV), deckt nur weniger wichtige, konkretisierende Bestimmungen<sup>25</sup>.

Eine Bestimmung, die den Bundesrat ausdrücklich ermächtigen würde, die Zulässigkeit der Internet-Überwachungen auf einzelne Kommunikationskanäle zu begrenzen, enthält das BÜPF nicht. Artikel 17 BÜPF wiederholt die Ausführungskompetenz des Bundesrats, ohne ihr etwas hinzuzufügen. Es bleibt daher nur Artikel 15 Absatz 6 BÜPF, wonach der Bundesrat «die Einzelheiten» zu bestimmen hat.

### 2.2.4.2 Wortlaut

Artikel 15 Absatz 6 BÜPF lautet:

«Der Bundesrat bestimmt die Einzelheiten. Wenn erforderlich kann er vorsehen, dass die Mitteilung kostenlos und rund um die Uhr zu erfolgen hat.»

«Le Conseil fédéral fixe les modalités d'application. Si nécessaire, il peut prévoir que la communication des données soit exécutée gratuitement et à n'importe quel moment.»

«Il Consiglio federale disciplina i dettagli. Se necessario, può prevedere che la comunicazione sia gratuita e abbia luogo 24 ore su 24.»

Der erste Satz gibt nach seiner Formulierung dem Bundesrat einen verbindlichen Regelungsauftrag. Der Gegenstand dieses Auftrags wird nicht spezifiziert, es geht pauschal um «die Einzelheiten». Ein solcher Auftrag ist immer in seinem Kontext zu interpretieren. Je nachdem ist er als Auftrag an den Bundesrat zu lesen, seine Ausführungsgesetzgebungskompetenz nach Artikel 182 Absatz 2 BV auch tatsächlich auszuüben. Der Begriff «Einzelheiten» lässt jedoch auch Raum für eine weitere Auslegung. Insbesondere können unter den Begriff der «Einzelheiten» sprachlich auch die einzelnen Überwachungstypen gefasst werden. Dies ist im vorliegenden Zusammenhang die plausiblere Interpretation, da nicht anzunehmen ist, dass der Gesetzgeber zunächst in Artikel 17 BÜPF den Bundesrat anhält, seine Ausführungsgesetzgebungskompetenz auszuüben, und dies dann in einem bestimmten Bereich wiederholt, ohne ihm etwas hinzuzufügen.

Der Wortlaut von Artikel 15 Absatz 6 BÜPF deckt somit die abschliessende, eingrenzende Regelung der Verordnung.

<sup>25</sup> Siehe statt vieler Pierre Tschannen, St. Galler Kommentar zu Art. 182 BV, Rz. 12 und 17–18.

### 2.2.4.3 Systematik

Die systematische Stellung in Artikel 15 BÜPF stellt klar, dass es nur um Einzelheiten anderer Regeln dieses Artikels gehen kann. Es fragt sich jedoch, ob nur alle oder nur bestimmte der in Artikel 15 enthaltenen Bestimmungen gemeint sind. Es wäre denkbar, dass Absatz 6 nur an Absatz 5 und den später eingefügten Absatz 5<sup>bis</sup> anknüpft, denn auf diese folgt er unmittelbar. Dafür spricht auch, dass mit bestimmten Artikeln (erster Satz: «die Einzelheiten»; zweiter Satz: «die Mitteilung») an bereits Genanntes angeknüpft wird. Insbesondere aufgrund der französischen Fassung wäre es naheliegend, nur den Bezug zu den Absätzen 5 und 5<sup>bis</sup> herzustellen, weil «la communication des données» in Absatz 5 und in Absatz 6 genau gleich formuliert ist, während die entsprechende Formulierung in Absatz 1 anders lautet: «transmettre les communications». Auch in den anderen Sprachen besteht eine Differenz zwischen «Mitteilung»/«comunicazione» (Abs. 5 und 6) und «zu[zur]leiten»/«trasmettere» (Abs. 1).

Allerdings ist es trotz dieser Indizien nicht ausgeschlossen, dass sich der sechste (heute genau genommen siebte) von acht (bzw. neun) Absätzen als Querschnittsbestimmung auf alle vorhergehenden Absätze bezieht. Dafür spricht, dass die darauf folgenden Absätze 7 und 8 eindeutig Querschnittscharakter haben.

Ebenfalls nicht auszuschliessen ist, dass sich der erste und der zweite Satz von Absatz 6 nicht auf dieselben Absätze beziehen. Davon hängen aber die dargestellten Überlegungen ab.

Aus systematischer Sicht ist es somit denkbar, dass sich der Auftrag, «die Einzelheiten» zu bestimmen, nur auf die Mitteilung der (wenigen) Angaben nach Artikel 14 Absatz 1 BÜPF bezieht. Es können jedoch sehr wohl auch Artikel 15 Absatz 1 und die dort genannte Weiterleitung des Fernmeldeverkehrs gemeint sein. Der wenig klaren Systematik des inhaltlich überfrachteten Artikels ist nicht zu viel Gewicht beizumessen.

### 2.2.4.4 Entstehungsgeschichte

Die Botschaft enthält zu Artikel 13 Absatz 5 des Entwurfs folgende Ausführungen:

«Nach Absatz 5 bestimmt der Bundesrat die Einzelheiten bezüglich Inhalt und Präsentationserfordernissen der Auskünfte und Übermittlungen von Anbieterinnen von Fernmeldedienstleistungen und die zeitliche Verfügbarkeit.» (BBI 1998 IV 4241, 4280)

«Selon le 5e alinéa, le Conseil fédéral définit les modalités concernant le contenu et la présentation des renseignements et transmissions fournis par les fournisseurs de services de télécommunication ainsi que les horaires de disponibilité.» (FF 1998 IV 3689, 3728)

Während «Übermittlungen» offen lässt, ob nur die mitzuteilenden Daten nach den Absätzen 5 und 5<sup>bis</sup> oder auch die Weiterleitung nach Absatz 1 gemeint sind, knüpft «transmissions» direkt an das Verb «transmettre» von Absatz 1 an. Die Formulierung «Inhalt (...) der Auskünfte und Übermittlungen» deckt eine Regelung der Zulässigkeit einzelner Überwachungstypen.

Aus den parlamentarischen Beratungen ergibt sich für diese Frage nichts<sup>26</sup>.

Aufgrund der französischen Version der Botschaft spricht die historische Auslegung somit dafür, dass der Bundesrat auch die «Einzelheiten» zu Absatz 1 regeln soll. Ob hingegen im Zusammenhang mit Absatz 1 eine Eingrenzung der zulässigen Überwachungstypen möglich sein soll, wird nicht klar.

### 2.2.4.5 Sinn und Zweck

Der Gesetzgeber kann weder schnell genug noch in einem genügenden technischen Detaillierungsgrad regeln, welche Überwachungstypen im Internet im Einzelnen zulässig sein sollen. Sinn und Zweck der gesamten Regelung muss unter anderem aber sein, die Rechtslage möglichst klar und vollständig zu gestalten. Verpflichtet das Gesetz somit die Internet-Anbieterinnen sehr pauschal, «den Fernmeldeverkehr» weiterzuleiten, so liegt der Schluss nahe, das Gesetz wolle mit den «Einzelheiten» auch eine präzise Regelung der zulässigen Überwachungstypen an den Bundesrat delegieren.

<sup>26</sup> Siehe Fussnote 18 zu Ziffer 2.2.2.3.

Dass dabei gegenüber dem gesamten Bereich «Fernmeldeverkehr» eine Einengung stattfinden kann, ist dieser Logik inhärent.

Die teleologische Auslegung spricht daher dafür, dass der Bundesrat gestützt auf Absatz 6 die Zulässigkeit der einzelnen Überwachungstypen im Internet regeln kann.

#### **2.2.4.6 Verfassungskonforme Auslegung und Bestimmtheitsgebot im Rahmen des Legalitätsprinzips**

Ginge man davon aus, dass im Internet-Bereich neben dem Katalog von Artikel 24 VÜPF direkt gestützt auf Artikel 15 Absatz 1 BÜPF noch weitere Überwachungstypen zulässig wären, so würde dies zu einem Konflikt mit dem Bestimmtheitsgebot führen, denn als Grundlage für die Verpflichtung der Anbieterinnen zur Weiterleitung des Internet-Verkehrs bliebe nur die sehr offene Formulierung von Artikel 15 Absatz 1 BÜPF: Die Anbieterinnen müssten dem Dienst «den Fernmeldeverkehr der überwachten Person» weiterleiten – mit den oben (2.2.2) dargestellten Unsicherheiten in der Auslegung. Der Katalog in Artikel 24 VÜPF hätte höchstens noch beispielhafte Bedeutung.

Das Bundesgericht formuliert die Anforderungen an die Bestimmtheit der gesetzlichen Grundlagen für Einschränkungen der Grundrechte wie folgt:

«Die Rechtsnorm soll so präzise formuliert sein, dass der Bürger sein Verhalten danach richten bzw. die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Gewissheit voraussehen kann. Dieses Erfordernis schliesst es nicht aus, dass ein Rechtssatz der anwendenden Behörde einen Beurteilungsspielraum einräumt, wenn das Ziel der Regelung hinreichend bestimmt ist, um eine angemessene Kontrolle der Handhabung der Norm zu ermöglichen. Der Gesetzgeber kann nicht völlig darauf verzichten, allgemeine Begriffe zu verwenden, die formal nicht eindeutig generell umschrieben werden können und die an die Auslegung durch die Behörde besondere Anforderungen stellen; denn ohne die Verwendung solcher Begriffe könnte er der Vielgestaltigkeit der Verhältnisse nicht Rechnung tragen.»<sup>27</sup>

Dass eine präzisere Umschreibung der zulässigen Überwachungstypen möglich ist, beweisen Artikel 24 VÜPF und der entsprechende Entwurf aus der Ämterkonsultation, der noch einen umfassenderen Katalog von Überwachungstypen enthielt und insbesondere die pauschale Weiterleitung des gesamten IP-Verkehrs einer Person deckte (s.o. Ziffer 2.2.3.3).

Da für viele Überwachungstypen ein grosser technischer Aufwand betrieben werden muss, ist es den Anbieterinnen nur schwer zuzumuten, bis zum Erhalt einer konkreten Überwachungsanordnung oder einer sonstigen Verfügung des Dienstes ÜPF im Unklaren gelassen zu werden, welche Überwachungstypen von ihnen verlangt werden.

Zudem ist zu beachten, dass die Regelung der Überwachungstypen tiefgreifende Auswirkungen auch auf die grundrechtlich geschützten Datenschutz-Interessen der Überwachten (Art. 13 BV) hat. Es ist von erheblicher Bedeutung, ob die Behörden nur den E-Mail-Verkehr abhören und bestimmte Randdaten einfordern oder ob sie jeglichen IP-Verkehr abhören können. Es ist zuzugestehen, dass im Strafprozess das anspruchsvolle Anordnungs- und Genehmigungsverfahren (Art. 6 ff. BÜPF) einen gewissen Schutz vor ungerechtfertigten Eingriffen bietet, der eine relative Offenheit der gesetzlichen Grundlagen ein Stück weit abzufedern vermag. Es kann jedoch nicht Ersatz sein für den fehlenden gesetzgeberischen Entscheid, ob aller Internet-Verkehr überwacht werden kann oder nur derjenige über E-Mail sowie gewisse Randdaten.

Vor diesem verfassungsrechtlichen Hintergrund wird das von der teleologischen Auslegung nahegelegte Resultat zwingend: Die gesetzgeberische Absicht muss gewesen sein, dass aus Gesetz und Verordnung insgesamt eine genügend bestimmte Regelung hervorgehen kann. Daher muss Artikel 15 Absatz 6 so gelesen werden, dass er den Bundesrat beauftragt, die zulässigen Überwachungstypen technisch präzise zu definieren. Dabei muss der Bundesrat sich selbstverständlich im Rahmen von Absatz 1 halten, kann daher aber auch den Bereich der zulässigen Überwachungstypen eingrenzen. Wortlaut, Systematik und Entstehungsgeschichte gehen teilweise auch in diese Richtung und erlauben dieses Resultat jedenfalls.

Im Unterschied zur Internet-Überwachung lag dem Kopfschaltungs-Entscheid des Bundesverwaltungsgerichts<sup>28</sup> eine genügende Regelung auf Verordnungsstufe (Art. 16 Bst. a VÜPF) zugrunde,

<sup>27</sup> BGE 125 I 361 E. 4.a S. 364. Siehe auch BGE 133 I 110 E. 6.1 S. 121.

<sup>28</sup> Bundesverwaltungsgericht, Entscheid A-2335/2008 vom 10. März 2009.

wonach die Echtzeit-Überwachung der Nutzinformationen<sup>29</sup> angeordnet werden konnte. Das Gericht musste bloss entscheiden, ob die Überwachung nur auf inländische oder auch auf ausländische Telefonanschlüsse fokussiert werden durfte.

### 2.2.4.7 Zwischenergebnis

Unseres Erachtens ist Artikel 15 Absatz 1 BÜPF zwar ein notwendiger Zwischenschritt auf dem gesetzgeberischen Weg zu einer rechtsstaatlich korrekten Verpflichtung der Zugangs-Anbieterinnen zur Weiterleitung des IP-Verkehrs. Alleine reicht er jedoch nicht. Er muss auf Verordnungsstufe präzisiert werden. Dies hat der Bundesrat in Artikel 24 VÜPF getan. Diese Bestimmung mit ihrer abschliessenden Aufzählung ist daher massgeblich.

### 2.2.5 Artikel 4 der TarifV als Grundlage?

Es wurde die Vermutung geäussert, möglicherweise finde sich eine gesetzliche Grundlage für die Verpflichtung der Anbieterinnen, den IP-Verkehr weiterzuleiten, in Artikel 4 TarifV. Dem kann das BJ nicht folgen. Diese Bestimmung erlaubt es dem Dienst, im Einzelfall Gebühren und Entschädigungen, für die keine pauschalen Ansätze bestehen, unter Berücksichtigung des Aufwands festzulegen. Dies kann zwanglos auf die fakultativen Aufgaben des Dienstes nach Artikel 13 Absatz 2 und Artikel 11 Absatz 2 BÜPF bezogen werden, denn auch für diese finden sich keine pauschalen Ansätze. Einen Rückschluss auf eine allfällige Verpflichtung der Anbieterinnen, bestimmte Leistungen zu erbringen, ermöglicht diese Bestimmung nicht. Ihr Thema ist nicht die Zulässigkeit von Massnahmen, sondern die Schaffung eines Auffangtatbestands für deren finanzielle Abgeltung.

### 2.2.6 Zwischenergebnis

Da der Bundesrat in Artikel 24 VÜPF nur einen kleinen Bereich der technisch möglichen Internet-Überwachungstypen für zulässig erklärt hat, verfügen im Internet-Bereich unseres Erachtens nur diese Überwachungstypen über genügende gesetzliche Grundlagen<sup>30</sup>.

Es ist zuzugeben, dass diese Regelung der VÜPF den heutigen Bedürfnissen der Strafverfolgung keineswegs entspricht. Die Regelung wurde aber so erlassen – und zwar unter Hinweis darauf, dass sie bald angepasst werden sollte<sup>31</sup>.

Es soll im Folgenden jedoch jeweils auch der Bereich ausserhalb des Katalogs geprüft werden, da unsere Auslegung offenbar nicht der bisherigen Praxis der Strafverfolgungsbehörden und des Dienstes ÜPF entspricht. Die nachfolgenden Überlegungen beruhen folglich auf der (unseres Erachtens unzutreffenden) Hypothese, mit Artikel 15 Absatz 1 BÜPF bestehe eine genügende gesetzliche Grundlage für solche Überwachungen.

## 2.3 Öffentliche und private Interessen

Die mit der Zwangsverpflichtung der Anbieterinnen einhergehenden Einschränkungen ihrer Wirtschaftsfreiheit müssen durch öffentliche Interessen oder durch den Schutz von Grundrechten Dritter gerechtfertigt sein (Art. 36 Abs. 2 und Art. 5 Abs. 2 BV).

<sup>29</sup> Die Nutzinformationen sind die eigentlichen Kommunikationsinhalte, z.B. das Telefongespräch selber; siehe die Erläuterungen vom 8. Oktober 2001 zur VÜPF, S. 8 (vgl. Ziffer 2.2.3.3).

<sup>30</sup> Im Ergebnis gleicher Ansicht, wenn auch jeweils ohne Begründung oder nur mit sehr knapper Begründung: Bundesstrafgericht BB.2009.4 vom 22. Juli 2009, E. 2.2.1; Jürg Schneider, Internet Service Provider im Spannungsfeld zwischen Fernmeldegeheimnis und Mitwirkungspflichten bei der Überwachung des E-Mail-Verkehrs über das Internet, AJP 2/2005, S. 179–192, 187; Thomas Hansjakob, Kommentar BÜPF/VÜPF, 2. Auflage St. Gallen 2006, Art. 24 VÜPF Rz. 4; Bernhard Sträuli, La surveillance de la correspondance par poste et télécommunication, in: Ursula Cassani u.a. (Hrsg.), Mehr Sicherheit – weniger Freiheit, Chur/Zürich 2003, S. 93–194, Rz. 188–189 S. 158 und Rz. 27 S. 104–105; Jean Treccani, Interceptions électroniques, in: Ursula Cassani u.a. (Hrsg.) a.a.O., S. 217–238, S. 228–229 und 236–237. Wohl auch in diesem Sinn August Biedermann, Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000, ZStrR 120 (2002), S. 77–106, 106.

<sup>31</sup> Siehe oben Ziffer 2.2.3.3.

An der Überwachung sowohl zur Aufklärung schwerer Straftaten (Art. 3 BÜPF) als auch zur Suche Vermisster (Art. 3a BÜPF) bestehen öffentliche wie auch private Interessen. Es besteht insbesondere ein grosses Interesse daran, dass alle zulässigen und angeordneten Überwachungen möglichst reibungslos abgewickelt werden können. Diese Interessen decken alle bisher diskutierten Auslegungsvarianten von Gesetz und Verordnung.

## **2.4 Verhältnismässigkeit**

### **2.4.1 Verhältnismässigkeit der Regelung**

Einleitend ist darauf hinzuweisen, dass hier nur geprüft werden kann, ob die *rechtlichen Grundlagen* der Verpflichtung der Internet-Anbieterinnen die Verhältnismässigkeit wahren. Diese ist aber ein Rechtsgrundsatz, der vor allem im konkreten Anwendungsfall seine Steuerungskraft entfaltet. Auch eine absolut angemessene Regelung kann in unverhältnismässiger Weise angewendet werden.

### **2.4.2 Eignung**

Mittels der Verpflichtung der Internet-Anbieterinnen zur Weiterleitung des IP-Verkehrs kann das Ziel erreicht werden, eine Überwachung des Internet-Verkehrs durchzuführen. Je weiter die Pflichten der Anbieterinnen gehen, umso leichter und reibungsloser dürften zudem im Allgemeinen die Überwachungen für die Behörden abzuwickeln sein. Die Eingriffe in die Rechte der Anbieterinnen erfüllen somit das Kriterium der Eignung grundsätzlich, unabhängig davon, welcher Auslegungsvariante der gesetzlichen Grundlagen man folgt.

### **2.4.3 Erforderlichkeit**

Das Kriterium der Erforderlichkeit besagt, dass keine mildereren Massnahmen verfügbar sein dürfen, die zur Verfolgung der öffentlichen und privaten Interessen gleich geeignet wären<sup>32</sup>.

Ohne alle technischen Details zu kennen, gehen wir davon aus, dass jede Minderung der Pflichten der Anbieterinnen tendenziell zu Mehraufwand und zur Erschwerung der Strafverfolgung führen kann. Daher scheint uns die Annahme vernünftig, dass auch sehr umfangreiche Verpflichtungen der Anbieterinnen das Kriterium der Erforderlichkeit erfüllen.

### **2.4.4 Interessenabwägung/Zumutbarkeit**

Der Aufwand und die Kosten, die den Anbieterinnen aus ihren Pflichten erwachsen, dürfen sie nicht allzu sehr belasten; die Einschränkungen müssen ihnen zumutbar sein<sup>33</sup>.

Die bisherige Rechtsprechung hat sich jeweils an zwei Regeln ausgerichtet: Erstens können die Fernmeldedienst-Anbieterinnen nicht verpflichtet werden, Massnahmen zu ergreifen, die ihnen subjektiv unmöglich sind (d.h. die zwar wohl im Rahmen des technisch Machbaren liegen, auf die die betreffende Anbieterin aber nicht vorbereitet ist)<sup>34</sup>.

Zweitens wurde der Aufwand für aussergewöhnliche Aufwendungen jeweils kostenorientiert entschädigt<sup>35</sup>.

Der Stellenwert der Überwachungen für die Strafverfolgung und die Suche Vermisster ist bekanntlich hoch, so dass mittels der beiden dargestellten Regelungen die Zumutbarkeit für die Anbieterinnen im Einzelfall vermutlich gewahrt werden kann.

<sup>32</sup> Rainer J. Schweizer, St. Galler Kommentar zu Art. 36 BV, Rz. 24.

<sup>33</sup> Rainer J. Schweizer, St. Galler Kommentar zu Art. 36 BV, Rz. 25.

<sup>34</sup> BGE 130 II 249 E. 2.2.2 und 2.2.3; Urteil des Bundesverwaltungsgerichts A-2335/2008 vom 10. März 2009, E. 3.1, 3.2 und 5; vgl. auch Urteil des Bundesverwaltungsgerichts A-2045/2006 vom 17. Februar 2009, E. 3.2.2.

<sup>35</sup> Urteil des Bundesgerichts 1A.255/2006 vom 20. März 2007, E. 3; Entscheid des Bundesstrafgerichts BB.2009.4 vom 22. Juli 2009 E. 2.2.

## 2.4.5 Zwischenergebnis

Wir können allgemein festhalten, dass die heutige Regelung es den Behörden insbesondere aufgrund der Entschädigung für besonderen Aufwand erlaubt, im Einzelfall die Verhältnismässigkeit gegenüber den Anbieterinnen zu wahren. Ob sich in Einzelfällen in besonderen technischen Konstellationen ein anderes Resultat ergäbe, können wir wie gesagt nicht beurteilen.

## 2.5 Gleichbehandlung der direkten Konkurrenten

Der Grundsatz der Gleichbehandlung der Konkurrenten verbietet Massnahmen, die den Wettbewerb unter direkten Konkurrenten verzerren bzw. nicht wettbewerbsneutral sind, namentlich wenn sie bezwecken, in den Wettbewerb einzugreifen, um einzelne Konkurrenten oder Konkurrentengruppen gegenüber anderen zu bevorzugen oder zu benachteiligen<sup>36</sup>. Der Grundsatz gilt jedoch nicht absolut und erlaubt es, aufgrund nicht wirtschaftspolitischer öffentlicher Interessen gewisse Unterschiede zu machen. Er geht allerdings weiter als das allgemeine Rechtsgleichheitsgebot: Er gewährt einen Schutz vor staatlichen Ungleichbehandlungen, die zwar auf ernsthaften, sachlichen Gründen beruhen mögen, gleichzeitig aber, ohne in der Hauptstossrichtung wirtschaftspolitisch motiviert zu sein, einzelne Konkurrenten namentlich durch unterschiedliche Belastungen oder staatlich geregelten Marktzugang bzw. -ausschluss begünstigen oder benachteiligen<sup>37</sup>.

Das heutige Recht der Fernmeldeüberwachung enthält keine Sicherungsmassregeln zur Verhinderung äusserst ungleicher technischer und zeitlicher Belastungen für die Fernmeldedienst-Anbieterinnen. So kann eine kleine Anbieterin, die etwa auf einem lokalen Kabelnetz den Internetzugang anbietet, von gleich aufwändigen Überwachungsmassnahmen betroffen sein wie ein landesweit tätiger, finanzstarker Konzern. Die Entschädigungen für die Anbieterinnen (Art. 16 Abs. 1 zweiter Satz BÜPF) federn diese faktische Benachteiligung heute jedoch deutlich ab, so dass unter dem heutigen Recht zumindest auf der Ebene der Einzelfall-Überwachungen allzu gravierende Ungleichheiten wohl vermieden werden.

Ohne die wirtschaftlichen Realitäten im Detail zu kennen, kann man daher vermuten, dass durch die Verpflichtung der Internet-Anbieterinnen zu aufwändigen technischen Überwachungsmassnahmen die Gleichbehandlung der direkten Konkurrenten nicht verletzt wird, weil die allenfalls ungleich verteilten Lasten finanziell zumindest teilweise abgegolten werden.

## 2.6 Ergebnis/Erfolgschancen

Nach der Ansicht des BJ genügt Artikel 15 BÜPF alleine nicht als gesetzliche Grundlage, um die Internet-Anbieterinnen zur Weiterleitung von Daten zu verpflichten. Vielmehr ist eine Konkretisierung auf Verordnungstufe erforderlich; diese kann auf Artikel 15 Absatz 6 BÜPF gestützt werden. In Artikel 24 VÜPF hat der Bundesrat die Konkretisierung vorgenommen. Dass diese Regelung zumindest heute nicht mehr zweckmässig ist, ändert daran nichts.

- Daher sind die Chancen als gut einzuschätzen, dass konkrete Überwachungsanordnungen im Internet-Bereich innerhalb des Katalogs von Artikel 24 VÜPF auch gegen den Willen der Anbieterinnen rechtlich durchgesetzt werden können.
- Hingegen dürften die Chancen gering sein, Internet-Überwachungen ausserhalb des Katalogs zwangsweise gegenüber den Anbieterinnen durchzusetzen. Nach der Ansicht des BJ sind diese Überwachungen unzulässig.

Auf dem Weg einer VÜPF-Revision könnten die Verpflichtungen im Rahmen des Gesetzes und der Verhältnismässigkeit ausgedehnt werden.

<sup>36</sup> BGE 125 I 431 E. 4.b.aa S. 435–36; siehe auch BGE 130 I 26 E. 6.3.3.1 S. 53; Urteil des Bundesverwaltungsgerichts A-2335/2008 vom 10. März 2009, E. 9.6; Klaus A. Vallender, St. Galler Kommentar zu Art. 27 BV, 2. Auflage 2008, Rz. 28.

<sup>37</sup> BGE 125 I 431.

### **3 Frage 1 (b): Verpflichtung der Internet-Anbieterinnen, sich technisch auf die Ausleitung des IP-Verkehrs vorzubereiten**

Hier ist zu prüfen, ob die Internet-Anbieterinnen gesetzlich verpflichtet sind, die nötigen technischen und organisatorischen Vorkehren zu treffen, um stets in der Lage zu sein, Weiterleitungen des IP-Verkehrs ihrer Kunden umgehend vorzunehmen. Falls diese Verpflichtung nicht direkt aus der Gesetzgebung hervorgeht, ist zu prüfen, ob sie den Internet-Anbieterinnen durch Verfügungen des Dienstes auferlegt werden kann.

#### **3.1 Grundrechtseingriff**

Zum Eingriff in die Wirtschaftsfreiheit und zum daraus resultierenden Prüfungsprogramm kann auf Ziffer 2.1.1 verwiesen werden. Die Schwere des Eingriffs akzentuiert sich dadurch, dass der Aufwand für die technische Vorbereitung nicht entschädigt wird (Art. 16 Abs. 1 erster Satz BÜPF).

#### **3.2 Gesetzliche Grundlage**

##### **3.2.1 Verpflichtung direkt gestützt auf die Gesetzgebung**

Aus den Artikeln 15 und 16 BÜPF kann man ableiten, dass das Gesetz – um eine praxistaugliche Überwachung sicherzustellen – die Fernmeldedienst-Anbieterinnen unausgesprochen verpflichtet, technisch jederzeit für die zulässigen Überwachungsmassnahmen gerüstet zu sein<sup>38</sup>. Wie schon bei der Teilfrage a stellt sich jedoch wieder das Problem, dass das BÜPF ein viel weiteres Feld von Überwachungsmassnahmen erfasst als die VÜPF: Die in Artikel 26 Absatz 1 VÜPF ausdrücklich normierte Vorbereitungspflicht erfasst nur die in Artikel 24 VÜPF aufgezählten Überwachungen. Nach der vorliegend vertretenen Auslegung des BÜPF und der VÜPF (s.o. 2.2) sind daher die Anbieterinnen nur verpflichtet, sich auf die Überwachungen gemäss dem Katalog von Artikel 24 VÜPF vorzubereiten.

Das Bestimmtheitsgebot im Rahmen des Legalitätsprinzips hat hier noch grösseres Gewicht als bei der Teilfrage a, weil die Anbieterinnen hier unabhängig von konkreten Einzelfällen und der damit zusammenhängenden Möglichkeit von Interessenabwägungen und der Gewährung des rechtlichen Gehörs (Art. 29 Abs. 2 BV) verpflichtet werden sollen. Dies verleiht der verfassungskonformen Auslegung von Artikel 15 Absatz 6 BÜPF zusätzliches Gewicht (s.o. Ziffer 2.2.4.6).

Eine verbindliche, generell-abstrakte Konkretisierung der Pflichten durch den Dienst ist nicht möglich, da der Dienst nicht über eine Gesetzgebungskompetenz verfügt (Art. 48 Abs. 2 RVOG, siehe Ziffer 2.2.1). Die technischen Richtlinien können daher auch hier nicht als gesetzliche Grundlage für die Verpflichtung der Anbieterinnen dienen<sup>39</sup>.

Die Erfolgchancen müssen daher ausserhalb des Katalogs von Artikel 24 VÜPF noch zurückhaltender eingeschätzt werden als bei der Frage 1 (a).

##### **3.2.2 Verpflichtung durch Verfügungen des Dienstes**

###### **3.2.2.1 Notwendigkeit gesetzlicher Grundlagen**

Auch für Verfügungen, die einzelne Anbieterinnen verpflichten würden, sich (etwa gemäss den technischen Richtlinien des Dienstes) auf bestimmte Überwachungstypen vorzubereiten, ist eine gesetzliche Grundlage notwendig<sup>40</sup>.

<sup>38</sup> Botschaft zum BÜPF, BBI 1998 IV 4121, 4280, zu Artikel 14 des Entwurfs.

<sup>39</sup> Bundesverwaltungsgericht, Entscheid A-2335/2008 vom 10. März 2009, E. 11.2.

<sup>40</sup> Siehe nur den Kopfschaltungs-Entscheid des Bundesverwaltungsgerichts, A-2335/2008 vom 10. März 2009, E. 7.3 und 7.4, wo für den Telefonbereich Artikel 15 Absatz 1 BÜPF i.V.m. Artikel 16 und 17 Absatz 1 VÜPF genügte.

### **3.2.2.2 Zulässigkeit von Verfügungen über die Vorbereitungspflicht**

Das BÜPF enthält keine ausdrückliche Regel, wonach der Dienst ÜPF die Anbieterinnen unabhängig von konkreten Überwachungen zu Vorbereitungshandlungen verpflichten könnte. Da die Verfügungsbefugnis in konkreten Überwachungsfällen geregelt ist (Art. 13 BÜPF und Art. 25 Abs. 1 VÜPF), könnte man im Umkehrschluss argumentieren, der Gesetzgeber habe auf die Möglichkeit präventiver Massnahmen des Dienstes bewusst verzichtet. Umkehrschlüsse sind jedoch stets genau zu prüfen, denn sie führen leicht zu Fehlüberlegungen. Dass die Verfügungsbefugnis in einer Sache genannt ist, heisst nicht unbedingt, dass sie in einer anderen Sache ausgeschlossen wird.

Überzeugender ist die Argumentation, aus der Stellung des Dienstes ÜPF als zuständiger Behörde des Bundes ergebe sich, dass der Dienst berechtigt sein müsse, die richtige Umsetzung des BÜPF und der VÜPF durch die Anbieterinnen zu überwachen und nötigenfalls mit juristischen Mitteln sicherzustellen. Die Bundesverfassung erlaubt es in Artikel 178 Absatz 3, Verwaltungsaufgaben auf Private zu übertragen, was das BÜPF durch die Verpflichtung der Anbieterinnen zur Durchführung der Überwachungen getan hat. Es ist nun in der Tat nicht anzunehmen, dass die Gesetzgebung den Privaten die Erfüllung staatlicher Aufgaben zwar rechtlich vorschreibt, den Behörden aber keine Möglichkeit gibt, juristisch auf einen korrekten Vollzug einzuwirken. Die Verfügungsbefugnis des Dienstes kann namentlich auch einer korrekten Handhabung der äusserst heiklen Personendaten dienen, die im Hinblick auf Überwachungen bearbeitet werden.

Daraus ist zu schliessen, dass die zuständige Behörde auch ohne ausdrückliche spezialgesetzliche Grundlage Verfügungen über die Vorbereitungspflicht erlassen kann. Das Bundesverwaltungsgericht hat im Telefonbereich eine entsprechende, auf künftige Überwachungen ausgerichtete Verfügung des Dienstes geschützt, ohne eine Gesetzesbestimmung zu verlangen, die solche präventiven Verfügungen ausdrücklich deckt<sup>41</sup>.

### **3.2.2.3 Materielle Grundlagen und Umfang der Verpflichtung**

Da sich die Verfügungskompetenz des Dienstes in Bezug auf die Vorbereitungspflicht der Anbieterinnen nur aus der materiellen Regelung herleiten lässt, muss sie sich auch in deren Rahmen bewegen. Die gesetzlichen Grundlagen für die Vorbereitungspflicht der Internet-Anbieterinnen umfassen nach der Ansicht des BJ, wie ausgeführt, nur den Katalog von Artikel 24 VÜPF (Teilfrage a). Könnte der Dienst durch Verfügungen den Geltungsbereich der gesetzlichen Grundlagen ausweiten, so liefe das auf eine Aushebelung des Legalitätsprinzips hinaus. Der Verordnungsgeber hat sich auf einen abschliessenden Katalog zulässiger Überwachungstypen festgelegt und muss sich nun darauf behaften lassen. Die gegenteilige Ansicht würde zudem eine Gefährdung der Rechtsgleichheit bedeuten, da die Privaten bei einer einzelfallweisen Festlegung der Pflichten durch eine Behörde schlechtere Gewähr dafür hätten, rechtsgleich behandelt zu werden.

### **3.2.2.4 Zwischenergebnis zur Verfügungsbefugnis des Dienstes**

Die Verfügungsbefugnis des Dienstes bezüglich technischer Vorbereitungsmaßnahmen kann aus der materiellen Regelung abgeleitet werden, sie muss daher aber deren Rahmen einhalten.

Auch hier sind aber die gesetzlichen Grundlagen dünn. Es sollte daher auch hier auf gesetzgeberischem Weg mehr Rechtssicherheit geschaffen werden.

### **3.2.3 Zwischenergebnis zu den gesetzlichen Grundlagen**

Innerhalb des Katalogs von Artikel 24 VÜPF sieht die Gesetzgebung eine Pflicht der Anbieterinnen vor, sich technisch auf Überwachungen vorzubereiten. Die Gesetzgebung deckt insbesondere auch Verfügungen des Dienstes ÜPF, welche die Pflichten einzelner Anbieterinnen konkretisieren.

Ausserhalb des Katalogs hingegen besteht keine Vorbereitungspflicht direkt gestützt auf die Gesetzgebung, und sie kann auch nicht auf dem Verfügungsweg neu eingeführt werden.

<sup>41</sup> Entscheid A-2335/2008 vom 10. März 2009, E. 6–10, betreffend Kopfschaltungen.

### 3.3 Öffentliche und private Interessen

Bezüglich der Interessenlage kann auf oben (2.3) verwiesen werden.

### 3.4 Verhältnismässigkeit

Ergänzend zu den Ausführungen oben (2.4) kann zur Verhältnismässigkeit Folgendes festgehalten werden:

Geht es um die Pflicht zur technischen Vorbereitung auf bestimmte Überwachungstypen, so liegt ein besonderes Gewicht einerseits auf der Schnelligkeit der Umsetzung konkreter Überwachungsanordnungen und andererseits auf den je nachdem enorm hohen Kosten für die Anschaffung oder Anpassung technischer Einrichtungen. Nur schon für den restriktiven Katalog von Artikel 24 VÜPF rechnete man für die grossen Anbieterinnen mit Investitionen in der Grössenordnung von einer Million Franken, und auch für die kleineren wurden Schätzungen von 50 000–100 000 Franken genannt<sup>42</sup>. Umso wichtiger sind angesichts dieser heiklen Interessenlage klare gesetzliche Grundlagen, wie sie für die Überwachung im Telefonbereich vorhanden sind und im Bereich des Internets fehlen.

Es versteht sich von selbst, dass das Kriterium der Zumutbarkeit einigen Spielraum eröffnet. Man könnte etwa argumentieren, das lukrative Geschäft der Zugangs-Anbieterinnen bestehe darin, einen Kommunikationskanal für alle möglichen Formen und Inhalte bereitzustellen, so dass es nur gerecht sei, sie auch an den daraus entstehenden Lasten zu beteiligen; daher müssten die Zugangs-Anbieterinnen auch sehr aufwändige Filtrierungs- und Aufbereitungsarbeit übernehmen. Dies überzeugt jedoch nicht. Man würde auch nicht von einem Camionneur erwarten, dass er den Inhalt der von ihm transportierten Container oder Paletten in- und auswendig kennt und jederzeit bereit ist, etwa bei Druckerzeugnissen detailliert und zielgenau Auskunft über bestimmte redaktionelle Inhalte zu erteilen. Wird der Absender einer Straftat verdächtigt, so muss es reichen, dass der Camionneur die Ware ablädt und gegebenenfalls die entsprechenden Pakete herausucht.

Wir können daher folgende Punkte festhalten:

- Die weitere Auslegung des Gesetzes (ohne Berücksichtigung der Verordnung), wonach die Zugangs-Anbieterinnen jegliche Kommunikationskanäle aus ihrem Datenstrom herausfiltern und aufbereiten müssen, würde mindestens in gewissen Fällen zu unzumutbaren Belastungen führen. Es ist nicht einzusehen, warum eine Anbieterin, die sich auf das technisch relativ simple Weiterleiten von IP-Datenpaketen beschränkt, für den Staat plötzlich ausgefeilte Filterungs- und Aufbereitungsarbeit übernehmen sollte. Gerade bei kleinen Anbieterinnen würde dies höchstwahrscheinlich zu unverhältnismässigen Belastungen führen.
- Die engere Auslegung des Gesetzes (ohne Berücksichtigung der Verordnung), wonach jede Anbieterin dem Staat ungefähr dieselben Dienstleistungen erbringen muss wie ihren Kunden, ist nach der Ansicht des BJ zumutbar. Der technische und finanzielle Aufwand dürfte sich für derartige Leistungen in einem vertretbaren Umfang halten – dies eine Vermutung aus der Laienperspektive. Ähnlich hat sich auch das Bundesverwaltungsgericht im Kopfschaltungsfall geäussert, wo es darum ging, dass die Anbieterin Telefonanrufe nach einem einfachen Kriterium, nämlich nach der Nummer des ausländischen Kommunikationspartners, ausfindig machen und weiterleiten musste<sup>43</sup>.
- Die Beschränkung auf den Katalog von Artikel 24 VÜPF dürfte umso mehr zu einer zumutbaren Belastung führen, wobei im Rahmen dieses Gutachtens auch hier keine detaillierte Prüfung vorgenommen werden kann.

Stets zu beachten ist jedoch, dass es sicher nicht verhältnismässig ist, eine Anbieterin bei ansonsten funktionierendem Geschäft durch die Pflicht zur technischen Vorbereitung in den Ruin zu treiben. Zudem sind die Interessen daran, die Last den Anbieterinnen aufzubürden, dort nicht besonders gewichtig, wo der Dienst ÜPF die technischen Aufgaben gut selber erfüllen könnte. Wie schon bei der

<sup>42</sup> David Rosenthal, Gesetz zur «Internet-Überwachung»: falsche Prioritäten?, Jusletter vom 3. Juni 2002, Rz. 8 / Neue Zürcher Zeitung, 31. Mai 2002.

<sup>43</sup> Bundesverwaltungsgericht, Entscheid A-2335/2008 vom 10. März 2009, E. 9.5.4.

Teilfrage a muss daher ein Vorbehalt angebracht werden für Einzelfälle, in denen es zu unzumutbaren Belastungen für die Anbieterinnen kommen könnte.

### **3.5 Ergebnis**

Wie bei der Teilfrage a sind die Chancen gering, die Internet-Anbieterinnen ausserhalb des Katalogs von Artikel 24 VÜPF zur technischen Vorbereitung auf die Überwachung des IP-Verkehrs zu verpflichten. Auf dem Weg einer VÜPF-Revision könnte diese Verpflichtung im Rahmen des Gesetzes und unter Wahrung der Verhältnismässigkeit ausgedehnt werden.

Innerhalb des Katalogs sind konkretisierende Verfügungen über die Pflichten der Anbieterinnen grundsätzlich zulässig.

## **4 Frage 1 (c): Tragung der Kosten der technischen Vorbereitung durch die Anbieterinnen**

Hier ist zu prüfen, ob die Internet-Anbieterinnen die Kosten der technischen und organisatorischen Vorbereitungsmaßnahmen gemäss Frage 1 (b) selber tragen müssen.

### **4.1 Artikel 16 BÜPF**

Artikel 16 Absatz 1 BÜPF auferlegt die Kosten der für eine Überwachung notwendigen Einrichtungen den Anbietern ohne Entschädigung; für die Kosten der einzelnen Überwachung hingegen spricht er ihnen eine angemessene Entschädigung zu. Dies wird in der Praxis so ausgelegt, dass die Anbieterinnen sämtliche Fixkosten selber tragen müssen, während die variablen Kosten zwar nicht voll, aber zu einem angemessenen Teil über die Entschädigungen gedeckt werden sollen<sup>44</sup>.

### **4.2 Innerhalb des Katalogs von Artikel 24 VÜPF**

Innerhalb des Katalogs von Artikel 24 VÜPF werden die Entschädigungen schematisch nach den Ansätzen von Artikel 2 TarifV bemessen. Der gesamte übrige Aufwand geht zulasten der Anbieterinnen. Der Bundesrat hat damit die Grundsatzregelung von Artikel 16 BÜPF in leicht handhabbarer, für das Massengeschäft tauglicher Form konkretisiert. Er konnte sich dafür auf Absatz 2 der Vorschrift stützen.

Diese Regelung schafft keine erkennbaren rechtlichen Grundsatzprobleme, weil die nötigen technischen Einrichtungen sich aus dem Katalog klar zu ergeben scheinen. Ob die Anbieterinnen aufgrund der in der Verordnung festgelegten Beträge für ihren Aufwand im Einzelfall angemessen<sup>45</sup> entschädigt werden, kann vorliegend aufgrund mangelnder Informationen über die finanziellen Verhältnisse nicht beurteilt werden.

### **4.3 Ausserhalb des Katalogs von Artikel 24 VÜPF**

Nach dem Gesagten (Teilfrage b) halten wir Überwachungsmaßnahmen ausserhalb des Katalogs für unzulässig. Die folgenden Erwägungen gehen von der Hypothese aus, dass die Verpflichtung zur technischen Vorbereitung von den Betroffenen im konkreten Fall nicht in Frage gestellt oder von den zuständigen Behörden bejaht wird.

<sup>44</sup> Urteil des Bundesverwaltungsgerichts A-2045/2006 vom 17. Februar 2009, E. 3.3.4; Urteil der REKO INUM J-2005-268 vom 25. Oktober 2006, E. 12; Urteil des Bundesstrafgerichts BB.2009.4 vom 22. Juli 2009, E. 2.2.2; Gutachten des BJ vom 16. Mai 2003 und vom 24. November 2003, Verwaltungspraxis der Bundesbehörden VPB 68.100.

<sup>45</sup> Zu den Kriterien siehe die in Fussnote 44 angegebenen Quellen.

Finden sich in der TarifV keine pauschalen Ansätze, so setzt der Dienst die Entschädigungen im Einzelfall je nach Aufwand durch den Dienst fest (Art. 4 TarifV). Dazu gibt ihm Artikel 16 Absatz 1 BÜPF die oben (Ziffer 4.1) dargestellte Vorgabe.

Diese Abgrenzung der Fixkosten von den variablen Kosten hat kaum eine Steuerungsfunktion, wenn der Dienst nach eigenem Dafürhalten bestimmt, welcher Aufwand im Voraus betrieben werden muss (d.h. welche Fixkosten generiert werden müssen). Verlangt man Einrichtungen, die für differenziertere Überwachungen konzipiert und dadurch teurer sind, so sinken die variablen Kosten und umgekehrt. Auch dies spricht dagegen, die Verpflichtung zur technischen Vorbereitung über den Katalog von Artikel 24 VÜPF hinaus zu anerkennen (Teilfrage b).

Zudem besteht ein weiteres Bestimmtheitsproblem, weil die TarifV keinen Stundenansatz für die Angestellten der Anbieterinnen nennt und auch sonst die Höhe der Entschädigungen offen lässt.

Die Praxis löste das Problem bisher so, dass Aufwendungen, die aus dem Rahmen des Katalogs fielen, nach einer möglichst realistischen Kostenrechnung entschädigt wurden<sup>46</sup>. Dazu mussten die Gerichte notgedrungen eigene Berechnungen anstellen und Ansätze aufstellen (etwa einen Stundenansatz von 160 Franken<sup>47</sup>). Dies ist jedoch suboptimal, weil erstens das Gesetz keine volle Kostendeckung, sondern bloss eine angemessene Entschädigung vorsieht, und zweitens das Problem der Abgrenzung von Fixkosten und variablen Kosten sich so nicht lösen lässt.

#### 4.4 Ergebnis

Obwohl die Rechtsprechung in Sonderfällen bisher stets aufgrund von Artikel 4 TarifV eine praktische Lösung gesucht hat, ist darauf hinzuweisen, dass die Bestimmtheit der gesetzlichen Grundlagen für die Festsetzung der Entschädigungen ausserhalb des Katalogs von Artikel 2 TarifV eigentlich ungenügend ist. Dies bringt ein gewisses Prozessrisiko mit sich, wenn Entschädigungsverfügungen des Dienstes angefochten werden.

### 5 Frage 2: Allfällige Überwälzung der Kosten auf die anordnenden Behörden

Zu prüfen ist, ob die bei den Anbieterinnen und beim Dienst ÜPF entstehenden Kosten – falls sie nicht von den Anbieterinnen getragen werden müssen – den anordnenden Behörden in Rechnung gestellt werden können.

Artikel 16 BÜPF schafft ein System, das es erlauben soll, die Aufgaben des Dienstes ÜPF für den Bund kostenneutral zu erfüllen<sup>48</sup>: Sämtlicher Aufwand soll entweder den Anbieterinnen verbleiben oder durch Entschädigungen und Gebühren der anordnenden Behörde auferlegt werden.

Überall, wo die TarifV einen pauschalen Ansatz enthält, ist dieser massgeblich; dies kann zu Abweichungen vom dargestellten Grundsatz der Kostendeckung führen. Wo kein pauschaler Ansatz besteht, hat die Praxis bisher stets kostenorientierte Gebühren und Entschädigungen zugesprochen.

Die Bestimmtheit der gesetzlichen Grundlagen der Kostenüberwälzung ausserhalb des Katalogs von Artikel 2 TarifV ist nach der Ansicht des BJ jedoch ungenügend (siehe oben zu Frage 1 c). Darin liegt ein gewisses Prozessrisiko.

<sup>46</sup> Entscheid des Bundesstrafgerichts BB.2009.4 vom 22. Juli 2009, E. 2.2.2; wohl auch Entscheid des Bundesgerichts 1A.255/2006 vom 20. März 2007, E. 3; Entscheid der REKO INUM J-2005-268 vom 25. Oktober 2006, E. 12.

<sup>47</sup> Entscheid des Bundesstrafgerichts BB.2009.4 vom 22. Juli 2009, E. 2.4.2, mit Hinweisen.

<sup>48</sup> Botschaft zum BÜPF, BBl 1998 IV 4241, 4280.

## 6 Frage 3: «Zertifizierung», «Compliance-Prozess»

Der Begriff «Zertifizierung» sollte vermieden werden, wo es darum geht, dass Private unfrei-willig von einer Behörde daraufhin kontrolliert werden, ob sie die Anforderungen der Gesetzgebung erfüllen, oder wo die Behörde Privaten verbindliche Anweisungen gibt, wie sie gesetzliche Pflichten umzusetzen haben.

Wir interpretieren die Ausführungen des Dienstes ÜPF so, dass er beabsichtigt:

- allen oder zumindest den wichtigen Fernmeldedienst-Anbieterinnen verbindliche Anweisungen zur Umsetzung der Vorbereitungspflicht (oben Frage 1 b) zu geben; und
- ein Prüfungsprogramm durchzuführen, um sicherzustellen, dass überall die Voraussetzungen gegeben sind, um Überwachungen jeder Art (nicht nur im Internet) durchführen zu können.

Zur Zulässigkeit dieses Vorhabens sind auf der aktuellen Abstraktionsstufe nur relativ allgemeine Aussagen möglich.

Zu Frage 1 (b) wurde ausgeführt, dass nach der Ansicht des BJ eine Pflicht der Anbieterinnen besteht, sich innerhalb der von der VÜPF gedeckten Bereiche technisch auf Überwachungen vorzubereiten, und dass auch konkretisierende Verfügungen über diese Vorbereitungspflicht zulässig sind. Ausserhalb der entsprechenden Kataloge<sup>49</sup> hält das BJ dies für unzulässig.

Zur Vollstreckung von Verfügungen stünden sodann die Massnahmen von Artikel 41 VwVG<sup>50</sup> zur Verfügung<sup>51</sup>, wobei die Ersatzvornahme und die Androhung von Ungehorsamsstrafen nach Artikel 292 StGB im Vordergrund stehen dürften (Art. 41 Abs. 1 Bst. a und d VwVG).

Dies deckt zumindest die zentralen Elemente des «Compliance-Prozesses» – aber eben nur im Rahmen der Kataloge in der VÜPF.

Das BJ empfiehlt daher, das «Compliance»-Projekt auf die Kataloge der VÜPF zu beschränken, es bis zum Inkrafttreten der oben empfohlenen VÜPF-Revision aufzuschieben oder es auf freiwilliger Basis weiterzuführen.

## 7 Exkurs: Beschwerdeberechtigung der Anbieterinnen

Mit Blick auf die Praxis sind hier noch Bemerkungen zur Beschwerdeberechtigung der Anbieterinnen anzubringen. Das Bundesgericht hat den Anbieterinnen ein Beschwerderecht gegen Anordnungen des Dienstes ÜPF in konkreten Überwachungsfällen nur in einem sehr engen Rahmen zuerkannt:

*«Les fournisseurs de services ne sont donc pas habilités à contester une décision du Service des tâches spéciales qui les oblige à transmettre des données couvertes par un ordre de surveillance dûment approuvé par l'autorité pénale compétente, en remettant en cause la légalité de cet ordre. Le recours institué en leur faveur à l'art. 32 OSCPT ne saurait donc porter sur ce point, mais uniquement sur des questions d'ordre technique ou organisationnel liées à l'exécution de la mesure de surveillance qui leur est demandée.*

*Pour le surplus, la question de savoir si les recherches par champ d'antennes sont ou non couvertes par la loi et son ordonnance d'application a trait à la légalité de la mesure de surveillance, dont l'examen ressortit à la compétence exclusive de l'autorité habilitée à autoriser la surveillance. Elle échappe ainsi au contrôle du Service des tâches spéciales et ne saurait être soumise à la cognition de la Commission de recours par le biais du recours prévu à l'art. 32 OSCPT, dans la mesure où les recourants ne prétendent pas que ce type de surveillance exigerait de leur part des connaissances ou des moyens techniques qui leur feraient défaut (...).» (BGE 130 II 249 E. 2.2.2, S. 255, Hervorhebungen hinzugefügt)*

Das Bundesgericht schloss somit ausdrücklich aus, dass die Anbieterinnen sich darauf berufen könnten, eine angeordnete Überwachungsmassnahme sei nicht zulässig. Dies sei nach der Konzeption des Gesetzes ausschliesslich Gegenstand des Strafprozesses. An diesem aber können sich die Anbieterinnen nicht beteiligen. Die Anbieterinnen können laut dem Bundesgerichtsentscheid nur technische und organisatorische Fragen rügen beziehungsweise geltend machen, dass sie nicht in der

<sup>49</sup> Art. 12 VÜPF für die Postüberwachung, Art. 16 VÜPF für die Überwachung des Fernmeldeverkehrs mit Ausnahme von Internet und Artikel 24 VÜPF für die Überwachung des Internet-Verkehrs.

<sup>50</sup> Bundesgesetz vom 20. Dezember 1968 über das Verwaltungsverfahren, SR 172.021.

<sup>51</sup> Siehe auch das Gutachten des BJ vom 31. Januar 2005, BJ-05-01-31, Verwaltungspraxis der Bundesbehörden VPB 70.46, Ziffer 3.4.2.3.

Lage seien, eine Überwachungsmassnahme auszuführen. In welchem Verhältnis die beiden Kriterien (technische/administrative Fragen oder Unmöglichkeit) stehen sollen, geht aus den Erwägungen nicht hervor. Der Entscheid bezieht sich zwar auf den Telefon-Bereich, es stellen sich bei Internet-Überwachungen aber dieselben Fragen<sup>52</sup>.

Interpretiert man diese Rechtsprechung eng, so führt sie für die Anbieterinnen zu einer unerträglichen Lage: Sie müssen gestützt auf Verfügungen des Dienstes ÜPF, die sich wiederum auf Anordnungen der Strafverfolgungsbehörden stützen, beliebig aufwändige technische Massnahmen ergreifen, doch können sie nicht gerichtlich überprüfen lassen, ob dafür genügende gesetzliche Grundlagen bestehen, ob die Verhältnismässigkeit gewahrt wird usw.

Das Bundesverwaltungsgericht hat sich im März des letzten Jahres differenziert mit dieser Rechtsprechung auseinandergesetzt und ist nach der Ansicht des BJ zu Recht zu folgendem Schluss gekommen:

«Wenn eine Fernmeldediensteanbieterin geltend machen kann, eine bestimmte Art der Überwachung fordere von ihr Kenntnisse und technische Mittel, über die sie nicht verfüge, so bedeutet dies, dass sie auch nicht in jedem Fall dazu verpflichtet werden kann, sich solche Kenntnisse und technische Mittel anzueignen. So muss sich eine Fernmeldediensteanbieterin dagegen wehren können, sehr hohe Investitionen für eine bestimmte Art der Überwachung des Fernmeldeverkehrs zu tätigen, sofern diese Art der Überwachung – unabhängig von einem konkreten Anwendungsfall – nicht rechtmässig ist.

3.4 Auf die Beschwerde ist nach den vorstehenden Erwägungen deshalb auch insofern einzutreten, als die Beschwerdeführerin rügt, ihr könne nicht zugemutet werden, die verlangten technischen Massnahmen umzusetzen, weil die damit ermöglichte Art der Überwachung nicht rechtmässig sei.»<sup>53</sup>

Das Bundesgericht hat sich seither nicht mehr mit der Frage der Beschwerdeberechtigung befasst, doch erscheinen die Überlegungen des Bundesverwaltungsgerichts als eine überzeugende Präzisierung gegenüber der etwas undifferenzierten Formulierung des Bundesgerichts.

Es ist also damit zu rechnen, dass den Anbieterinnen gegen Anordnungen des Dienstes ÜPF effektiver Rechtsschutz gewährt wird, insbesondere wenn sie fehlende Rechtsgrundlagen rügen.

## 8 Durchsetzung der richtigen Anwendung der Gesetzgebung durch die Bundesbehörden

Eine der Ursachen der heutigen, für den Dienst ÜPF unbefriedigenden Situation liegt darin, dass er Verfügungen von Strafverfolgungsbehörden durch eigene Verfügungen umsetzen und konkretisieren muss, auch wenn er selber von deren Unzulässigkeit überzeugt ist. Dies wiederum liegt daran, dass er als Verwaltungsbehörde nicht Entscheide richterlicher Behörden aufheben oder ändern kann. Sonst würde die Gewaltenteilung verletzt. Daher sind andere Wege zu prüfen, wie der Bund die richtige und einheitliche Umsetzung der Gesetzgebung im Bereich des BÜPF sicherstellen kann. Unseres Erachtens sollte die Option näher geprüft werden, ein Behördenbeschwerderecht gegen die Anordnungen der Strafverfolgungsbehörden einzuführen. Ein solches besteht heute nicht, könnte aber im Rahmen der BÜPF-Totalrevision neu verankert werden<sup>54</sup>. Es müsste insbesondere geprüft werden, an welche Rechtsmittelbehörde das Rechtsmittel führen könnte und ob es möglich und sinnvoll wäre, den Dienst ÜPF schon vor dem erstinstanzlichen richterlichen Genehmigungsentscheid anzuhören.

## 9 Empfehlungen für die Gesetzgebung

Fest steht, dass ein gesetzgeberisches Defizit besteht: Auf Gesetzesebene wird nicht im Detail geregelt (und lässt sich kaum im Detail regeln), welche technischen Massnahmen die Internet-Anbieterinnen ergreifen müssen und welche nicht. Auf Verordnungsebene findet sich eine für die Bedürfnisse der Praxis zu enge, abschliessend formulierte Aufzählung.

<sup>52</sup> Siehe auch Thomas Hansjakob, Kommentar BÜPF/VÜPF, 2. Auflage St. Gallen 2006, Art. 23 VÜPF, S. 461-464. Die Voraufgabe hatte noch für eine weitere Beschwerdeberechtigung der Anbieterinnen plädiert.

<sup>53</sup> Kopfschaltungs-Entscheid des Bundesverwaltungsgerichts, A-2335/2008 vom 10. März 2009, E. 3.3.2 und 3.4. Dieser Entscheid ist nach den Angaben Ihres Mitarbeiters Patrick Schöpf rechtskräftig.

<sup>54</sup> Parallel zu Art. 89 Abs. 2 Bst. a, Art. 76 Abs. 2 und Art. 81 Abs. 2 und 3 BGG.

Wir empfehlen Ihnen, zur Sanierung der Rechtslage folgenden Lösungsansatz zu verfolgen:

Gesetzesebene:

- Das BÜPF sollte im Rahmen der Totalrevision um eine Delegationsnorm ergänzt werden, wonach der Bundesrat die Überwachungstypen im Detail festlegt und dabei die technische und finanzielle Belastung für die Fernmeldedienst-Anbieterinnen berücksichtigt sowie sich am technischen Aufwand orientiert, den die Anbieterinnen privatautonom für ihre Kunden erbringen. Das Gesetz sollte vorsehen, dass der Bundesrat den Bereich der Überwachungsmaßnahmen, die strafprozessual zulässig sind, weiter ziehen kann als den Kreis der technischen Massnahmen, zu denen die Anbieterinnen verpflichtet werden. Der technische Aufwand, zu dem die Anbieterinnen nicht verpflichtet würden, müsste dann natürlich vom Staat übernommen oder auf vertraglich zu verpflichtende Drittunternehmen ausgelagert werden. Dies scheint sinnvoll, um auf technische Entwicklungen reagieren zu können, ohne die berechtigten Interessen der Anbieterinnen zu verletzen.
- Die Verfügungsbefugnis des Dienstes ÜPF sollte auch für die präventive Anordnung technischer Aufrüstungsmassnahmen ausdrücklich verankert werden.
- Es ist zu prüfen, ob gesetzliche Grundlagen für Zwangsmassnahmen gegenüber renitenten Anbieterinnen notwendig sind.
- Es ist zu prüfen, wie die Bundesbehörden die richtige und einheitliche Anwendung der Gesetzgebung sicherstellen können (siehe Ziffer 8).

Verordnungsebene:

- Die VÜPF sollte auf den aktuellen technischen Stand gebracht werden<sup>55</sup>. Nach der Ansicht des BJ erlaubt bereits das geltende Gesetz mit seinem weiten und unpräzisen Artikel 15 Absatz 1 und der Delegationsnorm in Absatz 6, dass der Bundesrat die zulässigen Überwachungstypen im Detail definiert und die Anbieterinnen verpflichtet, den Behörden Dienstleistungen im Umfang der privatautonom erbrachten Dienstleistungen zu erbringen. Die Aktualisierung der VÜPF sollte daher mit höchster Priorität vorangetrieben werden.
- Die TarifV sollte ebenfalls auf den aktuellen technischen Stand gebracht werden. Da offenbar auch andere als die in Artikel 24 VÜPF aufgezählten Internet-Überwachungstypen standardisiert durchgeführt werden sollen, sollten dafür Ansätze festgelegt werden. Zudem sollten für allfällige im Einzelfall zu bemessende Beträge möglichst Ansätze (etwa Stundenansätze) festgesetzt werden.

Dem Umstand, dass an einem Kommunikationsvorgang im Internet oft die verschiedensten Anbieterinnen von Teil-Leistungen beteiligt sind, ist stets besondere Aufmerksamkeit zu schenken. Es muss klar geregelt werden, welche Anbieterin welche Leistungen zugunsten der Behörden erbringen müssen.

Die Abgrenzung der Verantwortlichkeiten des Bundes beziehungsweise des Dienstes ÜPF und der Kantone muss im Auge behalten werden.

Schliesslich sind die Artikel 20 und 21 der Cybercrime-Konvention des Europarats<sup>56</sup> zu berücksichtigen, wonach sich die Mitgliedstaaten verpflichten, verschiedene Massnahmen zur Überwachung des Internet-Verkehrs zu ergreifen.

<sup>55</sup> Vgl. bereits die bei Jean Treccani, *Interceptions électroniques*, in: Ursula Cassani u.a. [Hrsg.], *Mehr Sicherheit – weniger Freiheit*, Chur/Zürich 2003, Fn. 37 S. 237 genannte Resolution der Conférence des autorités de poursuite pénale de la Suisse romande et du Tessin vom Herbst 2002.

<sup>56</sup> European Treaty Series No. 185, <http://conventions.coe.int> > Full list > 185; von der Schweiz signiert, aber noch nicht ratifiziert. Von März bis Juni 2009 wurde dazu eine Vernehmlassung durchgeführt, siehe [www.bj.admin.ch](http://www.bj.admin.ch) > Themen > Kriminalität > Gesetzgebung > Cybercrime

## **JAAC 2012.3 - Überwachung des Fernmeldeverkehrs – Pflichten der Dienstanbieterinnen bei Überwachungsmassnahmen im Internet**

In	Verwaltungspraxis der Bundesbehörden
Dans	Jurisprudence des autorités administratives de la Confédération
In	Giurisprudenza delle autorità amministrative della Confederazione
Jahr	2012
Année	
Anno	
Band	-
Volume	
Volume	
Seite	28-54
Page	
Pagina	
Ref. No	150 000 257

Das Dokument wurde durch das Schweizerische Bundesarchiv und die Bundeskanzlei konvertiert.  
Le document a été digitalisé par les Archives Fédérales Suisses et la Chancellerie fédérale.  
Il documento è stato convertito dall'Archivio federale svizzero e della Cancelleria federale.