Fernmeldeüberwachung à discrétion?

SIMON SCHLUARI *

Auf den 1. Januar 2012 setzte der Bundesrat neue Verordnungsgrundlagen zur Überwachung des Post- und Fernmeldeverkehrs in Kraft. Der vorliegende Beitrag beschäftigt sich mit den Neuerungen. Er hinterfragt insbesondere die Vorgehensweise des Bundesrates bei der Revision aus rechtsstaatlicher Sicht.

La révision de l'Ordonnance du Conseil fédéral sur la surveillance de la correspondance par poste et télécommunication est entrée en vigueur le 1er janvier 2012. L'article expose les nouvelles dispositions introduites par la révision. Il analyse en particulier l'attitude du Conseil fédéral adoptée lors de cette révision sous l'angle des règles de droit public.

I. Einleitung

Am 23. November 2011 verabschiedete der Bundesrat die revidierte Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)[1]. Sie wurde auf den 1. Januar 2012 in Kraft gesetzt, zeitgleich mit der ebenfalls revidierten Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF[2])[3].

Dieser Beitrag stellt einige wesentliche Neuerungen in diesen beiden Verordnungen vor. Er geht zudem der Frage nach, ob die Vorgehensweise des Bundesrates bei der Revision aus rechtsstaatlicher Sicht nicht etwas gar forsch war.

II. Warum die Revision?

Bundesrätin Simonetta Sommaruga eröffnete am 8. Juni 2011 ein Anhörungsverfahren für die geplante Revision der VÜPF und setzte einen entsprechenden Entwurf in Umlauf.

Als Grund für die Revision wurde in erster Linie angeführt, die Verordnung sei dem aktuellen Stand der Technik anzugleichen. Im Weiteren sei die Verordnung an die seit ihrem Erlass im Jahr 2001 er-

* PD Dr. iur., Rechtsanwalt. Der Autor arbeitet für Sunrise Communications AG. Der Text gibt ausschliesslich seine persönliche Auffassung wieder. Der Autor dankt lic. iur. CAROLINE AEBERLI, RA Dr. iur. MATTHIAS AMGWERD, RA lic. iur. MARCEL KÜCHLER, ANDREAS MEIER, Betriebsökonom FH, Dr. iur. CHRISTIAN TANNÒ und Dr. iur. ANJA TSCHIRKY für die kritische Durchsicht des Manuskripts.

[1] SR 780.11.
[2] SR 780.115.1.
[3] Die zugehörigen Materialien sind auf der Website des EJPD unter «Sicherheit»/«Überwachung des Post- und Fernmeldeverkehrs» abrufbar.

gangene Rechtsprechung anzupassen, und es sei notwendig, die neuen Überwachungsmassnahmen genügend bestimmt zu formulieren, um für alle Beteiligten die nötige Rechtssicherheit zu schaffen[4].

Bezüglich der Revision der GebV-ÜPF wurde dargelegt, die neuen Gebühren orientierten sich an der bestehenden Gebühren- und Entschädigungsstruktur. Eine Erhöhung werde nicht vorgeschlagen[5].

III. Bisherige Gerichtspraxis zu BÜPF und VÜPF

Seit dem Inkrafttreten des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und der zugehörigen ersten Version der VÜPF am 1. Januar 2002 ergingen einige wesentliche Gerichtsentscheide zum Themenkreis. Eine der zentralen Fragen war dabei jeweils, ob der Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF)[6] auf Anordnung von Strafverfolgungsbehörden auch die Schaltung von Überwachungstypen verfügen durfte, die weder im BÜPF noch in der zugehörigen Verordnung explizit geregelt waren.

1. Antennensuchlauf I

In BGE 130 II 249 lehnte das Bundesgericht einen Antrag der Swisscom ab, eine Verfügung des Dienstes ÜPF aufzuheben, mit der dieser von der Swisscom einen so genannten *Antennensuchlauf* verlangt hatte. Beim Antennensuchlauf geht es darum, sämtliche Verkehrsdaten, die in einer bestimmten Zeit in einer Mobilfunkzelle angefallen sind, rückwirkend bezüglich anrufender oder angerufener Telefonnummern zu durchsuchen.

Die Swisscom hatte argumentiert, die Anordnung von Antennensuchläufen sei unzulässig, weil damit – entgegen der eigentlichen Konzeption des BÜPF – nicht eine genau bestimmte Person aufgrund eines konkreten Verdachtsmoments überwacht werde, sondern eine unbestimmte Zahl von Personen ohne Verdachtsmoment. Auch sei die nachträgliche Information der überwachten Personen (heute in Art. 279 Strafprozessordnung geregelt) nicht gewährleistet. Entsprechend mangle es der Verfügung an einer genügenden gesetzlichen Grundlage.

Das Bundesgericht trat in der Folge allerdings gar nicht auf die Beschwerde der Swisscom ein. Es befand, die Anbieterinnen von Fernmeldediensten (FDA) seien zu einer Beschwerde gegen Verfügungen des Dienstes ÜPF nicht legitimiert, übernehme dieser doch nur eine Mittlerposition, in der er eine rein formelle Kontrolle der von den Strafverfolgungsbehörden erlassenen Überwachungsanordnungen ausübe. Eine materielle Kontrolle hinsichtlich der Rechtfertigung der Überwachungsmassnahme nehme der Dienst ÜPF nicht vor. Die Position der Swisscom unterscheide sich nicht von derjenigen der PTT nach dem früheren Gesetz. Dementsprechend sei auch die Swisscom nicht legitimiert, die gesetzliche Grundlage oder die Verhältnismässigkeit der angeordneten Überwachung gerichtlich überprüfen zu lassen. Die Frage, ob die konkret geforderten Antennensuchläufe zulässig seien, sei folglich einzig und allein durch das kantonale Massnahmengericht zu prüfen[7].

2. Kopfschaltung

Als Kopfschaltung bezeichnet man eine Überwachungsart, bei der sämtliche Gespräche überwacht werden, die von einem beliebigen Schweizer Anschluss aus auf einen bestimmten ausländischen Anschluss oder von diesem ausländischen Anschluss auf einen beliebigen Schweizer Anschluss getätigt werden.

In einem Entscheid des Bundesverwaltungsgerichts vom 10. März 2009[8] hatte dieses über die Beschwerde einer FDA zu entscheiden, die sich gegen eine Verfügung des Dienstes ÜPF zur Einrichtung einer Kopfschaltung richtete. Das Bundesverwaltungsgericht hiess die Beschwerde nur insoweit gut, als die betroffene FDA damals noch nicht in der Lage war, die Verbindungen eines ausländischen

---

[4] Zum Ganzen Dienst ÜPF, Erläuterungen (Entwurf) zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11) sowie Änderung der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1), 8. Juni 2011, www.ejpd.admin.ch/content/dam/data/pressemitteilung/2011/2011-06-08/1 10608_ber-de.pdf, 1 f.

[5] Dienst ÜPF (Fn. 4), 2.

[6] Der Dienst ÜPF führt auf Anordnung der Strafverfolgungsbehörden Post- und Fernmeldeüberwachungen durch; vgl. Art. 13 BÜPF.

[7] BGE 130 II 249, E. 2.2.2.

[8] BVGer vom 10. März 2010, A-2335/2008, «Kopfschaltung».

Telefonanschlusses mit ihren Netzwerken aktiv zu überwachen. Die FDA dürfe daher *nicht sofort* zu einer solchen Überwachung verpflichtet werden.

Als Begründung für ihre Beschwerde hatte die FDA angeführt, die Überwachung des Fernmeldeverkehrs erfolge gemäss Konzept des BÜPF an einem Anschluss (Konzept der Anschlussüberwachung). Eine Anschlussüberwachung könne die Beschwerdeführerin technisch bedingt nur durchführen, wenn die verdächtige Person einen Anschluss benutze, der zu ihren Netzen gehöre. Eine ausländische Rufnummer könne nicht mit einem Anschluss in den Netzen der Beschwerdeführerin in Verbindung gebracht werden[9]. Anders als bei einer normalen Überwachung werde nämlich genau besehen nicht ein einzelner Schweizer Anschluss überwacht, sondern es würden sämtliche Schweizer Anschlüsse überwacht. Für eine solche Verkehrsstromüberwachung finde sich im BÜPF jedoch keine genügende gesetzliche Grundlage.

Das Bundesverwaltungsgericht widersprach dem und fand, dem BÜPF sei keine Beschränkung auf in der Schweiz befindliche Anschlüsse zu entnehmen. Art. 15 BÜPF[10] bilde vielmehr zusammen mit Art. 17 Abs. 1 VÜPF[11] eine genügende gesetzliche Grundlage auch für eine Überwachung ausländischer Anschlüsse, wie sie bei einer Kopfschaltung erfolge.

Die Anordnung von Überwachungsmassnahmen sei zwar durchaus geeignet, in allfällige verfassungsmässige Rechte wie die Eigentumsgarantie und die Wirtschaftsfreiheit der Telekommunikationsunternehmungen einzugreifen. Es sei allerdings fraglich, wie weit FDA angesichts des noch immer weitgehend staatlich regulierten Marktes überhaupt legitimiert seien, sich auf diese verfassungsmässigen Rechte zu berufen[12].

Die Frage nach der Legitimation der FDA liess das Gericht in der Folge freilich offen, nachdem es festgehalten hatte, dass die Verpflichtung der FDA auf einer genügenden gesetzlichen Grundlage beruhe, im öffentlichen Interesse liege, verhältnismässig sei, und der Eingriff in die Grundrechte der Beschwerdeführerin damit im Lichte von Art. 36 BV ohnehin rechtmässig wäre[13].

3. Antennensuchlauf II

In einem Urteil vom 3. November 2011[14] hatte sich das Bundesgericht erneut mit einem Antennensuchlauf zu beschäftigen. Diesmal nahm es erstmals auch materiell zur Zulässigkeit Stellung.

Das Zwangsmassnahmengericht des Kantons Aargau hatte einen Antennensuchlauf zur Aufklärung von drei qualifizierten Raubüberfällen in Bijouteriegeschäften mangels dringenden Tatverdachts abgelehnt. Es führte insbesondere aus, der dringende Tatverdacht bilde eine der Voraussetzungen zur Durchführung einer Überwachungsmassnahme. Vorliegend liege aber das Ziel der Massnahme darin, einen Tatverdacht erst zu begründen.

Das Bundesgericht schützte demgegenüber die Position der Beschwerde führenden Staatsanwaltschaft Muri-Bremgarten mit einstimmigem Urteil: Einleitend legte das Gericht nochmals die Ordnung der Post- und Fernmeldeüberwachung in den Artikeln 269 ff. StPO dar: Zu unterscheiden sei zwischen a) einer inhaltlichen Überwachung des Fernmeldeverkehrs (Gespräche und Nachrichteninhalte) nach Art. 269 f. StPO, b) blossen Auskünften über Verkehrs- und Rechnungsdaten (bzw. Teilnehmeridentifikation) bei bekannten Teilnehmern bzw. Verdächtigen nach Art. 273 StPO sowie c) der gesetzlich nicht geregelten systematischen Rasterfahndung (Erhebung von Randdaten mittels eines Antennensuchlaufs) bei unbekannter Täterschaft[15]. Eine inhaltliche Überwachung sei dabei nur bei Delikten des Katalogs von Art. 269 Abs. 2 StPO zulässig, während Auskünfte über Verkehrs- und Rechnungsdaten nach Art. 273 Abs. 1 StPO bei Verbrechen und Vergehen generell sowie bei Missbrauch einer Fernmeldeanlage nach Art. 179^{septies} Strafgesetzbuch (die einzige Übertretung) eingeholt werden könnten.

---

[9] Vgl. Fn. 8, E. 7.1.
[10] Art. 15 Abs. 1 BÜPF statuiert die grundsätzliche Pflicht der FDA, Fernmeldeüberwachungen vorzunehmen.
[11] Gemäss Art. 17 Abs. 1 VÜPF bestimmt der Dienst ÜPF im Einzelfall die technischen und organisatorischen Massnahmen für die Durchführung der Überwachung.
[12] BVGer vom 10. März 2010, A-2335/2008, «Kopfschaltung», E. 9.1.
[13] Vgl. Fn. 12, E. 9.7.
[14] BGer vom 3. November 2011, 1B_376/2011, «Antennensuchlauf II».
[15] Vgl. Fn. 14, E. 5, Ingress.

In der Folge stimmte das Gericht der Lehrmeinung zu, dass Rasterfahndungen mittels eines Antennensuchlaufs grundsätzlich zulässig seien, allerdings nur zur Aufklärung *schwerer Delikte*, dass dabei der *Eingriff in die Rechte* der mitbetroffenen Unverdächtigen *minimal* zu halten sei, und dass die Gefahr, dass Unschuldige in ein Strafverfahren verwickelt werden könnten, gering sein, dass m.a.W. eine *eindeutige Selektion* erfolgen müsse. Was den erforderlichen dringenden Tatverdacht angehe, genüge bei Fahndungen gegen Unbekannt in solchen Konstellationen grundsätzlich bereits die *mögliche Individualisierbarkeit* der Zielpersonen gemäss Raster- bzw. Schnittmengenergebnis. Massnahmen *zu rein präventiven* Zwecken blieben indessen *unzulässig*.

Vorliegend rechtfertigte die Schwere der untersuchten Verbrechen laut Bundesgericht die streitige Überwachungsmassnahme. Bei der Schnittmengen-Ermittlung von Randdaten handle es sich sodann nicht um einen schweren Grundrechtseingriff, zumal die erhobenen Randdaten ja erst nach der Schnittmengenanalyse Personen zugeordnet würden (Selektion). Es sei zudem ausgeschlossen, dass viele Unbeteiligte in die zu ermittelnde Schnittmenge fallen würden (Individualisierbarkeit), und es sei angesichts der untersuchten Überfälle auch von einem dringenden Tatverdacht im genannten Sinne auszugehen. Der Antennensuchlauf sei zwar nicht explizit im Gesetz geregelt, die Verweigerung durch die Vorinstanz im vorliegenden Fall widerspreche aber dem Sinn und Zweck der Vorschriften zur Erhebung von Teilnehmeridentifikation sowie Verkehrs- und Rechnungsdaten (Art. 273 i.V.m. 269 Abs. 1 StPO).

4. Mobiles Internet

In zwei Entscheiden vom 21. bzw. 23. Juni 2011 betreffend Datenlieferungspflicht von Swisscom bzw. Sunrise[16] ging das Bundesverwaltungsgericht noch deutlicher von der Notwendigkeit einer gerichtlichen Überprüfung von Überwachungsmassnahmen auf Konformität mit den Grundrechten der FDA aus.

Sowohl die Swisscom als auch Sunrise waren durch den Dienst ÜPF verpflichtet worden, den Datenverkehr bestimmter Mobilfunkteilnehmer an den Dienst ÜPF auszuleiten. Beide FDA legten gegen die betreffende Verfügung Beschwerde ein. Auf den Entscheid zu Sunrise soll näher eingegangen werden.

Sunrise machte geltend, für die verlangte Überwachungsart fehlten eine genügende gesetzliche Grundlage bzw. ein genügend bestimmter Rechtssatz. Insbesondere sei die Aufzählung der möglichen Überwachungsmassnahmen gemäss Art. 24 VÜPF abschliessend zu verstehen.

Anders als beim erwähnten BGE 130 II 249 anerkannte das Bundesverwaltungsgericht zunächst die Legitimation von Sunrise, gerichtlich gegen Verfügungen des Dienstes ÜPF vorzugehen[17]. Dies gestützt auf Art. 48 Abs. 1 Verwaltungsverfahrensgesetz, gemäss dem u.a. zur Beschwerde berechtigt ist, wer durch die angefochtene Verfügung berührt ist und ein schutzwürdiges Interesse an deren Aufhebung oder Änderung hat. Sunrise könne sich dagegen wehren, sich Kenntnisse oder Mittel aneignen zu müssen und sehr hohe Investitionen für eine bestimmte Art der Überwachung zu tätigen, sofern diese Art der Überwachung – unabhängig von einem konkreten Anwendungsfall – nicht rechtmässig sei[18].

Sodann hielt das Gericht fest, der Dienst ÜPF habe seine Verfügung zwar zu Recht nicht auf Art. 24 VÜPF gestützt, denn die verlangte Überwachungsart sei in jener Norm nicht geregelt. Indessen fehle der Verfügung auch sonst die vom Gesetzgeber in Art. 15 Abs. 6 BÜPF verlangte Konkretisierung auf Verordnungsstufe, weshalb sie über keine genügend bestimmte gesetzliche Grundlage verfüge. Die Beschwerdeführerin könne daher zurzeit nicht zum Erwerb der für die Überwachung des mobilen Internetverkehrs notwendigen Einrichtungen gezwungen werden[19].

Ferner liess sich das Gericht obiter über die nach seiner Ansicht dringende Notwendigkeit einer Verordnungsrevision aus.

---

[16] BVGer vom 21. Juni 2011, A-8284/2010, «Swisscom»; BVGer vom 23. Juni 2011, A-8267/2010, «Sunrise».
[17] Auch die Legitimation von Swisscom wurde, anders als in BGE 130 II 249 (vorne III.1), nicht mehr in Frage gestellt; BVGer vom 21. Juni 2011, A-8284/2010, «Swisscom», E. 1.3.
[18] BVGer vom 23. Juni 2011, A-8267/2010, «Sunrise», E. 1.3.
[19] Vgl. Fn. 18, E. 3.3.4; zum gleichen Schluss kommt auch das Bundesamt für Justiz, Pflichten der Dienstanbieterinnen bei Überwachungsmassnahmen im Internet, 16. April 2010, www.bfm.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/gutachten-buepf-uepf-d.pdf, 13 ff.

IV. Einige wesentliche Neuerungen im Überblick

1. Persönlicher Geltungsbereich

a) Internetanbieter versus Internetzugangsanbieter

Der Entwurf zur neuen VÜPF vom Juni 2011 war hinsichtlich des persönlichen Geltungsbereichs sehr offen gehalten: Insbesondere sollten auch reine Anbieter von Internet*anwendungen,* wie Internettelefonie (Skype u.dgl.) oder Instant-Messaging (wie Whatsapp), einer Überwachungspflicht unterstellt werden. Dies ist u.a. daraus ersichtlich, dass der Entwurf im französischen Verordnungstext von Art. 1 Abs. 2 lit. e den Begriff «fournisseurs *d'accès à* Internet» noch durch den Begriff «fournisseurs Internet» ersetzen wollte[20].

Nachdem in der Vernehmlassung diesbezüglich mehrheitlich Kritik geübt worden war[21], beschränkt sich die definitive Fassung der Verordnung nun auf Zugangsanbieter, wie aus Art. 1 Abs. 2 lit. e ersichtlich ist: Die Rede ist jetzt – wie seit jeher im französischen Text – von Internet*zugangs*anbieterinnen und nicht mehr von Internetanbieterinnen.

Aufatmen dürften insbesondere Betreiber von Webseiten mit Kommunikationsfunktionen (wie Foren, Blogs u.dgl.), überraschte doch das Bundesgericht in einem höchst fragwürdigen[22] Entscheid vom 8. Januar 2010 einen Forenbetreiber bös und verurteilte diesen wegen Begünstigung, weil er die IP-Adressen[23] seiner Nutzer nicht aufgezeichnet hatte[24]. Dieser Praxis wurde mit der Verordnungsrevision jetzt ein Riegel geschoben.

b) Problematische Differenzierung bezüglich Überwachung von Internetanwendungen

Die Überwachung von Internetanwendungen ist allerdings nicht ganz aus der Welt: Gemäss dem neuen Art. 24 Abs. 2 VÜPF werden nämlich doch bestimmte Anwendungen überwachungspflichtig. Mit der neuen Regelung in Art. 1 Abs. 2 lit. e VÜPF betrifft diese Überwachungspflicht aber nur noch Anwendungsanbieter, die zugleich Zugang zum Internet offerieren[25].

Diese neue Ungleichbehandlung zwischen Zugangsanbietern und reinen Anwendungsanbietern ist heikel: So ist beispielsweise Apple als reine Anwendungsanbieterin nicht verpflichtet, für den kürzlich eingeführten Instant-Messaging-Dienst «iMessage» eine Überwachung vorzusehen. Eine Überwachungspflicht entstünde auch dann nicht, wenn sie diese Funktion neu auf der Set-Top-Box des Video-on-Demand-Produkts «Apple TV» einführte.

Entscheidet sich nun aber eine Schweizer FDA, bei ihrem Video-on-Demand-Angebot eine ähnliche Funktion einzuführen (etwa eine Chatfunktion, über die man sich mit anderen Nutzern austauschen kann), so wäre die FDA im Gegensatz zu Apple dazu verpflichtet, ihre Set-Top-Boxen an die Infrastruktur des Dienstes ÜPF anzubinden. Zu überwachen wären sodann etwa auch Chat-Funktionen auf den Webseiten der FDA oder Diskussionsforen zur Verbesserung des Kundendienstes.

Die dabei anfallenden Kosten dürften die Anreize der FDA, mit derartigen Funktionen zu experimentieren, nachhaltig schmälern und insbesondere die in letzter Zeit verstärkten Bemühungen der FDA, auch in Märkte für Internetanwendungen vorzustossen, erschweren. Zudem bietet nur ein kleiner Teil

[20] Dienst ÜPF, Erläuterungen (Entwurf; vorne Fn. 4), 7.
[21] Dienst ÜPF, Bericht über das Ergebnis des Anhörungsverfahrens, September 2011, www.ejpd.admin.ch/content/dam/data/sicherheit/ uepf/ve-ber-d.pdf, 3; vgl. etwa auch Schweizerischer Verband der Telekommunikation asut, Stellungnahme zur Anhörung zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs, asut.ch/files/pdf1035.pdf?2173, 4.
[22] Anders noch Verfahrensgericht Basel-Landschaft, Beschluss Nr. 440 09 67 vom 1. April 2009, E. 7; kritisch zum Bundesgericht A. BACHMANN, Bundesgericht, Strafrechtliche Abteilung, Urteil vom 8. Januar 2010 i.S. Y gegen Staatsanwaltschaft des Kantons Aargau – 6B_766/2009, forumpoenale 2010, 346 ff., 348, m.d.H.
[23] IP-Adressen sind Adressen von Geräten in Computernetzen, die auf dem Internetprotokoll (IP) basieren.
[24] BGer vom 8. Januar 2010, 6B_766/2009.
[25] Dienst ÜPF, Erläuterungen zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11) sowie Änderung der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1), 26. Oktober 2011, www.bfm.admin.ch/content/dam/data/sich erheit/uepf/vn-ber-d.pdf, 2; zu den überwachten Anwendungen hinten IV. 4.

der Anwendungsanbieter zugleich auch Internetzugang an, womit nur ein kleiner Ausschnitt aus der riesigen Angebotsvielfalt überhaupt überwachungspflichtig wird.

Entsprechend muss in Frage gestellt werden, ob die neu eingeführte Ungleichbehandlung mit den Grundsätzen der Rechtsgleichheit (Art. 8 BV) und der Wettbewerbsneutralität staatlichen Handelns (Art. 94 Abs. 1 BV) vereinbar ist.

2. Öffnung des Katalogs der Überwachungsmassnahmen

Wie erwähnt hat das Bundesverwaltungsgericht im Entscheid vom 23. Juni 2011 (Terminierung Mobilfunk) die Einführung der neuen, in der VÜPF nicht geregelten Überwachung des mobilen Internetverkehrs abgelehnt. Dies mit der Begründung, laut Art. 15 Abs. 6 BÜPF habe der Bundesrat die Einzelheiten der Überwachung zu regeln, und der gestützt auf diese Delegationsnorm in Art. 24 VÜPF festgelegt Katalog von Überwachungsmassnahmen sei demnach abschliessend zu verstehen[26]. Die Auffassung des Dienstes ÜPF, wonach neue Überwachungsarten unmittelbar auf Art. 15 BÜPF gestützt eingeführt werden könnten, gehe fehl, weil das Gesetz so präzise formuliert sein müsse, dass der Bürger sein Verhalten danach richten könne (Grundsatz des genügend bestimmten Rechtssatzes[27]). Gleiches müsse auch für FDA gelten, gerade weil die Überwachung als technisch sehr anspruchsvolle Aufgabe zu gelten habe[28].

Mit den neuen Art. 17 Abs. 5 und 25 Abs. 5 VÜPF führt der Verordnungsgeber nun aber zwei Bestimmungen ein, die genau dieses soeben erst gerichtlich bestätigte Regime der alten VÜPF auf den Kopf stellen: Plötzlich sollen auch Überwachungsarten möglich sein, die nicht in der Verordnung oder im Gesetz aufgeführt sind.

Diese Vorgehensweise führt zunächst einmal die erklärte Absicht des Verordnungsgebers ad absurdum, auf Seiten der FDA und auch beim potenziell von einer Überwachung betroffenen Bürger für mehr Rechtssicherheit zu sorgen[29]. Im Gegenteil muss nun jederzeit mit neuen Überwachungsarten gerechnet werden, während die alte VÜPF klare Grenzen setzte.

Dazu kommt, dass der Gesetzgeber in Art. 15 Abs. 6 BÜPF eine Delegation allein an den Bundesrat vorgenommen hat. In einem solchen Fall bleibt zwar eine Subdelegation an ein Departement zulässig (Art. 48 Abs. 1 Regierungs- und Verwaltungsorganisationsgesetz), indes hätte die Subdelegation an den dem Eidgenössischen Justiz- und Polizeidepartement (EJPD) unterstehenden Dienst ÜPF[30] eine zusätzliche Ermächtigung durch ein Bundesgesetz oder einen allgemeinverbindlichen Bundesbeschluss vorausgesetzt (Art. 48 Abs. 2 RVOG)[31].

Erst recht muss es auch unzulässig sein, einer Behörde unterhalb der Departementsstufe die Kompetenz zu *Einzelfallentscheiden* ganz ohne genügend bestimmte generell-abstrakte Rechtsgrundlage zu verleihen, wie dies in Art. 17 Abs. 5 und Art. 25 Abs. 5 VÜPF geschieht. Dies ergibt sich aus dem besprochenen Entscheid vom 23. Juni 2011 (Mobiles Internet), wonach dem es einer Verfügung des Dienstes ÜPF, die nicht auf einer in der VÜPF konkretisierten Verpflichtung beruht, an einer genügenden gesetzlichen Grundlage fehlt, weil nach Art. 15 Abs. 6 BÜPF *der Bundesrat* die Einzelheiten zu regeln hat[32].

Weil zudem der Dienst ÜPF, wie das Bundesgericht im Entscheid «Antennensuchlauf I» festhielt, nach der Konzeption von BÜPF und StPO selber keine Entscheidungskompetenz hat, sondern die Anfragen der Strafverfolgungsbehörden nur in rein formeller Hinsicht zu kontrollieren und an die FDA weiterzuleiten hat, nimmt der Bundesrat mit Art. 17 Abs. 5 und Art. 25 Abs. 5 VÜPF faktisch sogar eine Delegation des Entscheids zur Einführung neuer Überwachungstypen an die kantonalen Strafverfolgungsbehörden vor. Diese sind aber grundsätzlich stets daran interessiert, neue Überwachungstypen einzuführen, und deshalb denkbar ungeeignet, über diese Frage zu entscheiden.

---

[26] BVGer vom 23. Juni 2011, A-8267/2010, «Sunrise», E. 3.3.
[27] Dazu statt vieler U. HÄFELIN/W. HALLER/ H. KELLER, Schweizerisches Bundesstaatsrecht, 7. Aufl. Zürich 2008, N 308.
[28] Vgl. Fn. 26, E. 3.3.1.
[29] Vgl. Dienst ÜPF, Erläuterungen (Fn. 25), 2.
[30] Art. 3 Abs. 1 VÜPF.
[31] Vgl. auch schon Bundesamt für Justiz (Fn. 19), 8; zur Subdelegation allgemein T. GÄCHTER, in: G. Biaggini/T. Gächter/R. Kiener (Hg.), Staatsrecht, Zürich 2011, § 22 N 38; T. SÄGESSER, Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997, Stämpflis Handkommentar, Bern 2007, RVOG 48 N 5 f.
[32] BVGer vom 23. Juni 2011, A-8267/2010, «Sunrise», E. 3.

Ferner hätte der Bundesrat selbst vor einer nach Art. 48 Abs. 1 RVOG zulässigen Delegation an ein Departement die Tragweite der entsprechenden Normen zu berücksichtigen gehabt (Satz 2 der Bestimmung), m.a.W. hätte er bei wesentlicher Tragweite auf eine Subdelegation verzichten müssen[33]. Dabei hat der Bundesrat Rechtssetzungsaufgaben von u.a. wesentlicher politischer oder sozialer Tragweite selber wahrzunehmen und darf sie nicht auf Verwaltungseinheiten übertragen.[34] Angesichts des Gefährdungspotenzials, das von einer ungezügelten Fernmeldeüberwachung auf einen freiheitlichen Rechtsstaat und seine Bürger ausgeht, und angesichts der politischen Brisanz des Themas wäre damit wohl selbst eine Subdelegation der Auswahl der Überwachungstypen an das EJPD problematisch gewesen[35].

Dass die Endfassung der Verordnung, anders als noch der Entwurf, die Einführung neuer Überwachungsarten jeweils auf Fälle beschränkt, in denen die benötigten Schnittstellen bei den FDA bereits vorhanden sind, ändert an der grundlegenden Problematik wenig: Die Schnittstelle stellt regelmässig nur ein kleines Element der gesamten für eine Überwachungsart benötigten Infrastruktur dar. Zudem werden die fraglichen Schnittstellen ohnehin universell genutzt, d.h. grundsätzlich können alle Arten von Daten übertragen werden.

Es ist damit fraglich, ob die in Art. 17 Abs. 5 und 25 Abs. 5 VÜPF vorgenommene Öffnung des Katalogs der Überwachungsmassnahmen vor den Gerichten Bestand haben wird.

3. Kopfschaltung und Antennensuchlauf

Kopfschaltung und Antennensuchlauf sind neu in den Artikeln 16b bzw. 24c sowie 16 lit. e VÜPF kodifiziert. Gemäss Bundesrat handelt es sich dabei wie erwähnt[36] um eine blosse Nachführung, mit der die Verordnung um durch die Rechtsprechung ohnehin bereits bewilligte Überwachungsarten ergänzt wurde.

Über die Zulässigkeit des Antennensuchlaufs hatte das Bundesgericht indessen – wie beschrieben[37] – bis kurz vor dem Erlass der neuen Verordnung wegen Nichteintretens gar nie materiell entschieden, sodass nicht von einer Nachführung die Rede sein konnte. Und auch die Kopfschaltung wird durch den neuen Art. 24c VÜPF deutlich über die bisherige Gerichtspraxis hinaus ausgedehnt: Neu soll auch die Überwachung ausländischer Internetanschlüsse[38] sowie von SMS[39] möglich sein, während bisher einzig die Überwachung ausländischer Telefonanschlüsse gerichtlich genehmigt worden war[40]. Entsprechend ist es auch hier nicht korrekt, von einer blossen Nachführung zu sprechen[41].

4. Internetüberwachung

Das eigentliche Herzstück der Revision bilden die Neuerungen im Bereich der Internetüberwachung: Während diese bisher in einer einzigen Bestimmung (Art. 24 VÜPF) geregelt und im Wesentlichen auf den E-Mail-Dienst beschränkt war, wird sie neu in den vier ausführlichen Art. 24, 24a, 24b und 24c VÜPF geregelt.

Art. 24 Abs. 1 VÜPF regelt neu die *Arten von Internetzugängen,* die überwacht werden sollen. Während bisher nur Festnetz-Internetanschlüsse überwacht wurden (auch dies bisher ohne genügende Verordnungsgrundlage, denn wie die Überwachung mobiler Internetanschlüsse[42] war die Überwachung von Festnetz-Internetanschlüssen in der alten VÜPF nicht geregelt), sind neu auch Internetanschlüsse über Mobilfunk (lit. c), solche über WLAN (lit. d), andere Zugänge via OSI-Schicht 2 (wie Glasfaser; lit. e) sowie Zugänge via OSI-Schicht 3 (wie Virtual Private Networks, VPN; lit. f) zu überwachen.

---

[33] SÄGESSER (Fn. 31), RVOG 48 N 9 f.
[34] SÄGESSER (Fn. 31), RVOG 48 N 1.
[35] Dies wäre auch einer allfälligen Position entgegen zuhalten, gemäss der die Kompetenzerteilung an den Bundesrat zur Subdelegation an den Dienst ÜPF in ungeschriebener Form im Gesetz enthalten sei; zu dieser Möglichkeit grundsätzlich SÄGESSER (Fn. 31), RVOG 48 N 23.
[36] Vorne II.
[37] Vorne III.1 und III.3.
[38] Art. 24c VÜPF; Dienst ÜPF, Erläuterungen (Fn. 25), 12 f.
[39] Art. 16b i.V.m. Art. 16 lit. a VÜPF; Dienst ÜPF, Erläuterungen (Fn. 25), 6.
[40] Der Dienst ÜPF, Erläuterungen (Fn. 25), 12, schliesst von der bundesgerichtlichen Erlaubnis für die Überwachung von Telefonanschlüssen ohne Weiteres auf eine solche für Internetanschlüsse.
[41] Vgl. auch asut (Fn. 21), 10.
[42] Vorne III.4.

Wie erwähnt regelt Art. 24 Abs. 2 VÜPF zusätzlich die Überwachung von Internet*anwendungen.* Betroffen sind asynchrone und synchrone Postdienste wie E-Mail oder Instant Messaging sowie auf digitalen Medien beruhende Fernmeldedienste*.* Zu den Letzteren gehören Internetanwendungen wie Voice-over-IP oder andere Audio- oder Videoübertragungen. Wie beschrieben[43] gilt die Pflicht, Internetanwendungen zu überwachen, nach der Endfassung der Verordnung nurmehr ausschliesslich für Unternehmen, die auch Internetzugang anbieten. Reine Anwendungsanbieter wie Skype sind damit von der Überwachungspflicht neu ausgenommen[44].

Art. 24a VÜPF regelt detailliert die Überwachung in Echtzeit, Art. 24b VÜPF die rückwirkende Überwachung. Rückwirkend bedeutet dabei, dass die FDA verpflichtet sind, die bei der Kommunikation ihrer Kommunikationsteilnehmer anfallenden Adressierungselemente für sechs Monate zu speichern und auf Anfrage des Dienstes ÜPF bzw. der Strafverfolgungsbehörden herauszugeben[45].

In *Echtzeit* zu überwachen sind zunächst sämtliche über einen Anschluss übermittelten Daten (Art. 24a lit. a VÜPF) bzw. bei Überwachung von Anwendungen deren Nutzinformationen (Art. 24a lit. c VÜPF). *Sowohl bei Echtzeit- als auch bei rückwirkender Überwachung* sind Datum und Uhrzeit bereitzustellen, zu der die Datenverbindung hergestellt und getrennt wird bzw. wurde, sodann die Art der Verbindung oder des Anschlusses, die verwendeten Log-in-Daten[46], verfügbare Adressierungselemente[47], Kommunikationsparameter wie IMEI-Nummer, MAC-Adresse u.dgl. sowie beim Zugang über Mobilfunknetze die Parameter der aktiven Antenne[48] (Art. 24a lit. b bzw. Art. 24b lit. a VÜPF). Bei synchronen Internetanwendungen wie Instant Messaging ist die Übermittlung von Randdaten nur bei Echtzeitüberwachung vorgesehen (Art. 24a lit. d VÜPF), bei asynchronen wie E-Mail – wie bisher – auch bei der rückwirkenden Überwachung (Art. 24b lit. b VÜPF).

Beide Bestimmungen erfassen also fast jeden erdenklichen Kommunikationsparameter. Es geht somit auch an dieser Stelle nicht um eine blosse Nachführung bzw. Anpassung der Verordnung an die bisherige Gerichtspraxis, sondern um eine *massive Ausdehnung der Überwachung.* Der Bundesrat geht offenbar davon aus, dass Art. 15 Abs. 1 BÜPF, der die FDA im Sinne eines Grundsatzes zur Überwachung verpflichtet, selbstverständlich auch eine mehr oder minder vollständige Überwachung des Internetverkehrs und insbesondere auch der Internetanwendungen umfasst.

Man kann sich allerdings aus heutiger Sicht mit Recht fragen, ob dem Gesetzgeber beim Erlass des BÜPF vor elf Jahren wirklich eine derart allumfassende Internetüberwachung vorschwebte. Immerhin stammt das BÜPF, so das Bundesamt für Justiz (BJ), «aus einer Zeit, als zumindest in den meisten Köpfen bei der Überwachung des Fernmeldeverkehrs noch relativ klar war, was überwacht wurde: Telefongespräche, Faxdokumente, Telexnachrichten usw. Das Internet war noch eine neue, zwar boomende, aber in den Details nur wenig bekannte Erscheinung»[49]. Die Frage war damals weniger, welche Dienste des Internets zu überwachen waren, sondern vielmehr, ob das Internet *überhaupt* überwacht werden sollte[50].

Dazu kommt, dass das BÜPF seiner Konzeption nach nicht eine schrankenlose Überwachung billigt, sondern – neben dem grundrechtlichen Schutz der betroffenen Bürger vor ungerechtfertigten Eingriffen in die Privatsphäre[51] – auch einen Interessenausgleich zwischen FDA und Strafverfolgungsbehörden bezweckt[52]. Die nun vorgenommene massive Ausweitung der Internetüberwachungsarten stört

[43] Vorne IV.1.a).
[44] Bislang wurden Anwendungen wie Skype bekanntlich ohne gesetzliche Grundlage durch Installation eines «Bundes-Trojaners» überwacht; vgl. etwa T. HANSJAKOB, Einsatz von GovWare – zulässig oder nicht?, Jusletter, 5. Dezember 2011. Der Einsatz eines Trojaners bildet zudem Gegenstand der kommenden Revision des BÜPF. Zu dieser wiederum etwa M. A. KESSLER/B. ISENRING, Die geplante Total-Revision des BÜPF im Überblick, Sicherheit&Recht 2011, 24 ff.; vgl. auch Bundesamt für Justiz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens, Mai 2011, www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/ fernmeldeueberwachung/ve-ber-d.pdf.
[45] VÜPF, Anhang (Art. 2), Ziff. 4.
[46] Der Begriff *Log-in-Daten* kann sich dabei einzig auf die zum Aufbau der Verbindung zwischen Kunde und FDA verwendeten Log-in-Daten beziehen, nicht aber auf Log-in-Daten für Anwendungen, die nicht der Überwachung unterstehen (etwa E-Banking oder nicht durch die FDA betriebene VoIP-Dienste). Alles andere würde den Delegationsrahmen der Verordnung sprengen.

[47] Dazu sogleich mehr im Abschnitt IV.5.
[48] Zu Letzteren die Kritik bei asut (Fn. 21), 6.
[49] Bundesamt für Justiz (Fn. 19), 11.
[50] Bundesamt für Justiz (Fn. 19), 11.
[51] Dazu hinten IV.5.a).
[52] So auch das Gutachten des Bundesamtes für Justiz (Fn. 19), 12.

diesen Interessenausgleich zumindest insofern, als die FDA zugleich eine empfindliche Einbusse bei der finanziellen Abgeltung für ihre Arbeiten hinnehmen müssen[53].

Schliesslich geht die Verordnung gerade im Bereich der Überwachung von Internetanwendungen über das hinaus, was in der Europäischen Union durch die Vorratsdatenspeicherungsrichtlinie 2006/24/EG gefordert wird, beschränkt sich die Richtlinie doch auf E-Mail und Internettelefonie.

Es ist zwar nachvollziehbar, dass heute die Überwachung von E-Mail allein nicht mehr ausreicht, um eine effiziente Strafverfolgung zu gewährleisten. Doch aus dem offen formulierten Wortlaut von Art. 15 Abs. 1 BÜPF zu schliessen, der Gesetzgeber habe dem Bundesrat schon im Jahr 2000 einen Freibrief für die nun vorgenommene massive Ausweitung der Überwachung gegeben, dürfte zu weit gehen[54]. Entsprechend unsicher ist, ob die Gerichte die vier neuen Normen wirklich zur Anwendung zulassen werden.

5. Rückwirkende Überwachung der verfügbaren Internet-Adressierungselemente

Bei der rückwirkenden Überwachung der verfügbaren Internet-Adressierungselemente ist eine neue Bestimmung besonders heikel, die sich – man möchte beinahe sagen: gut versteckt – in Art. 24b lit. a Ziff. 4 VÜPF findet. Gemäss dieser Norm kann die *rückwirkende Übermittlung der verfügbaren Adressierungselemente* angeordnet werden, und zwar insbesondere der Adressierungselemente des *Ursprungs der Kommunikation*.

a) Offener Begriff der Adressierungselemente

Die Problematik liegt hier im Begriff der *Adressierungselemente:* Bei diesen handelt es sich um *Kommunikationsparameter* sowie *Nummerierungselemente* wie Kennzahlen, Ruf- und Kurznummern. Kommunikationsparameter sind Elemente zur Identifikation u.a. von Personen oder Maschinen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind[55]. Der Begriff ist damit offen. Er umfasst insbesondere auch IP-Adressen und könnte aufgrund seines Wortlaut sogar so weit verstanden werden, dass auch *Uniform Resource Locators (URLs),* also die präzisen Adressen der Webseiten, die ein Teilnehmer über seine Internetverbindung abruft[56], erfasst werden[57].

b) Faktische rückwirkende Überwachung von Internet-Inhalten

Insbesondere bezüglich der IP-Adressen ist zu beachten, dass *jeglicher* Internetverkehr unter Verwendung von solchen abgewickelt wird: Alle Kommunikationsinhalte werden digitalisiert und in Datenpakete aufgeteilt. Diese Datenpakete werden in der Folge mit der IP-Adresse von Absender und Empfänger versehen und über mehrere Knotenpunkte des Netzes bis zum Zielrechner weiter gereicht. Geht es um Inhalte des World Wide Web, ist zudem immer eine URL im Spiel.

Weil Webseiten oft *statisch* sind (d.h. identische Adressen liefern auch nach längerem Zeitablauf dieselben Inhalte), lässt sich anhand einer einmal aufgezeichneten IP-Adresse oder URL oft auch der übertragene Inhalt rekonstruieren. Damit kann gestützt auf Art. 24b lit. a Ziff. 4 VÜPF faktisch eine rückwirkende Überwachung der Kommunikations*inhalte* des Internets erfolgen; dies im Gegensatz zur Überwachung von Telefon-Randdaten, bei der kaum Rückschlüsse auf den Inhalt von Gesprächen gezogen werden können.

---

[53] Dazu unten Abschnitt IV.6.
[54] Anders Generalsekretariat GS-EJPD, Revision des BÜPF und der VÜPF, Medienrohstoff, www.bfm.admin.ch/content/dam/data/sicherheit/uepf/mr_buepf_vuepf-de.pdf, demgemäss man der Auffassung ist, das Parlament sei nicht umgangen worden.
[55] Vgl. VÜPF, Anhang (Art. 2), Ziff. 9 und Art. 3 lit. g Fernmeldegesetz; dazu P. R. FISCHER/O. SIDLER, in: R. H. Weber (Hg.), Schweizerisches Bundesverwaltungsrecht, Bd.V: Informations- und Kommunikationsrecht, Teil 1: Allgemeiner Überblick, Fernmelderecht, Presse- und Filmverwaltungsrecht, 2.Aufl., Basel 2003, N 266.
[56] Wie www.sic-online.ch.
[57] Nach Art. 2 i.V.m. Art. 3 FMG stellen insbesondere Internetdomainnamen Adressierungselemente dar; FISCHER/SIDLER (Fn. 55), N 285.

c) Beschränkung durch den gesetzlichen Delegationsrahmen

Damit geht Art. 24 b lit. a Ziff 4 VÜPF klar über den vom Gesetzgeber in Art. 15 BÜPF gesteckten Delegationsrahmen hinaus. Die Materialien ergeben zwar wenige Hinweise; indessen ist anzunehmen, dass der historische Gesetzgeber einer (auch rein faktischen) rückwirkenden Speicherung von Inhalten nicht zugestimmt hätte, sondern dass er sich auf Randdaten beschränken wollte, die keine Rückschlüsse auf Inhalte zulassen. Dies entspräche ganz dem Konzept von BÜPF und Art. 269 ff. StPO, die keine anlasslose Überwachung von Inhalten vorsehen[58]. Der Anwendungsbereich von Art. 24b lit. a Ziff. 4 VÜPF muss also schon aufgrund des von Art. 15 BÜPF gesteckten Delegationsrahmen beschränkt werden.

Ähnliches ergibt sich sodann auch aus dem Entscheid «Antennensuchlauf II», gemäss dem eine Rasterfahndung ohne dringenden Tatverdacht der überwachten Personen nur anhand von Randdaten, nicht aber anhand der übermittelten Inhalte vorgenommen werden darf[59].

Wie auch die Videoüberwachung[60] bedürfte eine rückwirkende Überwachung von Inhalten damit einer zusätzlichen formell-gesetzlichen Grundlage.

d) Fehlende Grundlage in Verfassung

Zu beachten ist sodann der verfassungsrechtliche Rahmen, den insbesondere die Meinungs- und Informationsfreiheit des Bürgers nach Art. 16 BV bzw. Art. 10 EMRK und sein Recht auf informationelle Selbstbestimmung (Datenschutz) nach Art. 13 BV bzw. Art. 8 EMRK stecken. Dieser würde durch eine flächendeckende rückwirkende Überwachung von Internetinhalten zweifellos gesprengt: Wie das deutsche Bundesverfassungsgericht festhielt, ist bereits eine Überwachung von Randdaten geeignet, «ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann»[61]. Dies muss erst recht für eine anlasslose Speicherung von Inhalten gelten[62], die damit aus verfassungsrechtlicher Sicht nicht zu tolerieren ist.

Anders als Bundesgesetze (Art. 190 BV) sind Verordnungen des Bundesrates nicht vor einer Verfassungsmässigkeitsprüfung durch die Gerichte geschützt. Zumindest solange der gesetzliche Delegationsrahmen einer verfassungskonformen Auslegung zugänglich ist, hat sich der Bundesrat an die Verfassung zu halten. Art. 15 BÜPF bzw. Art. 24b lit. a Ziff. 4 VÜPF sind demnach verfassungskonform auszulegen, was ebenfalls auf eine Reduktion des jeweiligen Sinnes gegenüber dem zu weiten Wortlaut hinausläuft.

e) Lösungsvorschlag

Auch das auf den ersten Blick einengend zu verstehende Tatbestandsmerkmal «insbesondere des Ursprungs» ändert an dem zu weiten Wortlaut der Norm genau besehen nichts:

Erstens ist der Begriff des Ursprungs für Internetkommunikation aus technischer Sicht undefiniert. Wenn der Kommunikationsteilnehmer eine Internetverbindung aufbaut, indem er beispielsweise eine Webseite aufruft, so sendet sein Rechner zunächst eine Anfrage an den Server, auf dem diese gespeichert ist. Dieser antwortet in der Folge mit den gewünschten Inhaltsdaten, also dem eigentlichen Inhalt der Webseite. Damit bleibt unklar, ob mit dem Begriff «Ursprung» die Adressdaten des Rechners des Teilnehmers oder jene des Webservers gemeint sind.

Zweitens wird zudem die Einfügung durch die Formulierung «insbesondere» ohnehin faktisch ihrer Wirkung beraubt, denn damit wären eben nicht mehr nur die Ursprungsadressen, sondern auch

[58] Vgl. BGer vom 3. November 2011, 1B_376/2011, E. 5, und dazu vorne III.3.
[59] Dazu vorne III.3.
[60] Dazu BGer vom 13. Oktober 2010, 1C_315/2009, «Echtzeit-Videoüberwachung», E. 2.2.
[61] Urteil des deutschen Bundesverfassungsgerichts vom 2. März 2010, 1 BvR 256/08, N 212.
[62] Eine anlasslose Kenntnisnahme der besuchten Webseiten ist nicht einmal in einem privaten Arbeitsverhältnis zulässig, in das sich der Arbeitnehmer freiwillig begeben hat. Entsprechend enger müssen die Grenzen im öffentlichen Recht sein. Zur Überwachung im Arbeitsverhältnis etwa S. WOLFER, Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis, Zürich 2008 = Diss. Luzern 2008, N 507.

Zieladressen von den FDA rückwirkend zu speichern und auf Anfrage des Dienstes ÜPF herauszugeben.

Eine Hilfestellung zur Korrektur des Problems mag aber eine weniger technische Interpretation des Begriffs «Ursprung» bieten: Versteht man ihn nicht in dem genannten technischen Sinn, sondern so, dass es der Kunde des FDA ist, der die Kommunikation mit einem Server *initiiert* (Ursprung der Kommunikation), so kann die Norm dahingehend interpretiert werden, dass zwar Kommunikationsparameter *auf Kundenseite* (etwa die IP-Adresse des Kunden) aufgezeichnet werden sollen, nicht aber Kommunikationsparameter von Gegenstellen, m.a.W. also nicht die durch den Kunden aufgerufenen Serveradressen und insbesondere nicht die übermittelten URLs. Dem entspricht nicht zuletzt auch die Darstellung in den Erläuterungen des Dienstes ÜPF, der als Beispiel für den Ursprung der Kommunikation die Rufnummer eines Mobiltelefons nennt, von dem aus eine Internetverbindung aufgebaut wird[63].

6. Änderungen an der Gebührenverordnung

Ein weiterer Kritikpunkt bei der Anhörung betraf die Gebühren, mit denen die Strafverfolgungsbehörden die FDA für ihre Überwachungstätigkeit entschädigen[64]. Sie sind wie beschrieben in der genannten Gebührenverordnung GebV-ÜPF geregelt, die gleichzeitig mit der VÜPF revidiert wurde. Der Bundesrat beabsichtigte mit der Revision eine Kostensenkung für die Strafuntersuchungsbehörden[65].

Während von Seiten der Strafverfolgungsbehörden eine deutliche Reduktion der Gebühren gefordert worden war (diese seien prohibitiv hoch, ja sogar höher als in jedem anderen westeuropäischen Land, und Überwachungsmassnahmen dürften nicht an den anfallenden Gebühren scheitern[66]), wehrten sich die FDA gegen die «Kostensenkung», die aus ihrer Perspektive natürlich auf eine Erhöhung der eigenen Beiträge an die Gesamtheit der Überwachungskosten hinausläuft[67].

Die bestehenden Pauschaltarife gemäss neuer GebV haben sich gegenüber der Verordnung aus dem Jahre 2004 nicht verändert. Indessen werden vor allem die Aufträge zur Überwachung von Datendiensten neu pauschal und nicht mehr nach Aufwand entschädigt, was zu Ausfällen führen wird. Zudem bleibt abzuwarten, wie sich die Zahl der Überwachungsanfragen angesichts der erweiterten Möglichkeiten der Strafverfolgungsbehörden entwickeln wird.

Angesichts dessen, dass die Überwachung massiv ausgeweitet wurde, was zu erheblichen Investitionen seitens der Provider Anlass geben wird, bringt dies den erwähnten, vom Gesetzgeber gewollten Interessenausgleich zwischen Strafverfolgungsbehörden und FDA womöglich aus dem Lot. Zu begrüssen ist immerhin, dass der Bundesrat im Hinblick auf die kommende BÜPF-Revision eine Erhebung über die bei den FDA tatsächlich anfallenden Kosten für die Überwachung in Auftrag gegeben hat.

7. Behandlung kleiner Anbieterinnen von Fernmeldediensten

In der Schweiz gibt es neben den grossen FDA noch weit über hundert kleinere betroffene FDA, insbesondere im Bereich Internet[68]. Diese beschäftigen oftmals deutlich unter zehn Personen.

Gerade aus den Reihen dieser kleinen FDA kam insofern harsche Kritik am Entwurf für die neue VÜPF, als dieser die Überwachung massiv ausweitete, von den FDA aber zugleich die Sicherstellung der Überwachung auch ausserhalb der Bürozeiten verlangte (vgl. Art. 18 Abs. 3 und Art. 26 Abs. 3 VÜPF).

Der Dienst ÜPF hat mittlerweile zumindest die Absicht geäussert, bei kleinen FDA, die durch eine Pikettpflicht rund um die Uhr überfordert wären, von einer Pflicht zur Reaktion ausserhalb der Bürozeiten abzusehen. Zudem sollen die kleinen FDA nicht verpflichtet werden, auf Vorrat teure Überwa-

[63] Dienst ÜPF, Erläuterungen (Fn. 25), 9.
[64] Vgl. insbesondere asut (Fn. 21), 11.
[65] Vgl. etwa Dienst ÜPF, Erläuterungen (Fn. 25), 18.
[66] Dienst ÜPF, Bericht (Fn. 21), 4.
[67] Der Deckungsgrad der staatlichen Beiträge im Vergleich zu den Gesamtkosten der Überwachung beträgt nach Angaben der FDA bisher nur rund 30%; vgl. asut (Fn.21), 11.
[68] Sie organisieren sich in der Swiss Network Operators Group SwiNOG, vgl. www.swinog.ch, und neuerdings im Verband SwiNOG Federation.

chungsinfrastruktur zu beschaffen. Vielmehr soll der Dienst ÜPF weiterhin selber Infrastruktur installieren, sollte es bei einem solchen Anbieter einmal zu einer Überwachung kommen[69].

Zusammenfassung

Dass die VÜPF seit ihrem Erlass im Jahr 2001 in die Jahre gekommen war und ihre Funktion angesichts des technischen Fortschritts nicht mehr wirklich zu erfüllen vermochte, leuchtet ein. Abgesehen von wenigen Teilaspekten wie E-Mail enthielt die Verordnung insbesondere keine Regelung für die Überwachung des Internets. Dennoch verlangte der Dienst ÜPF von den Anbieterinnen von Fernmeldediensten (FDA) auch diese. Die FDA kamen diesem Wunsch zumindest im Festnetzbereich bisher nach. Gegen eine neue Forderung, auch Internetverbindungen über Mobilfunk zu überwachen, wehrten sie sich indessen erfolgreich mit dem Argument, die Verordnungsgrundlage sei ungenügend. Die neue Verordnung behebt diesen Mangel und sorgt insofern für mehr Rechtssicherheit.

Zu Kritik gibt nun aber Anlass, dass die Revision der VÜPF deutlich über das hinaus geht, was angekündigt war, nämlich eine Angleichung der Verordnung an die seit ihrer Inkraftsetzung ergangene Rechtsprechung und die besagte Anpassung an den technischen Fortschritt. Dass der Bundesrat – auch angesichts der politischen Brisanz des Themas Überwachung – eine solche Ausweitung vornahm und nicht auf die in Kürze ohnehin geplante Revision des BÜPF[70] warten mochte, um die Angelegenheit dem demokratisch legitimierten Gesetzgeber zu überlassen, ist bedauerlich, wenn nicht rechtsstaatlich fragwürdig.

Dazu kommt, dass – entgegen der kürzlich durch das Bundesverwaltungsgericht bestätigten Rechtslage – nicht mehr nur der Bundesrat, sondern neu auch der Dienst ÜPF selber – und mit ihm indirekt die kantonalen Strafverfolgungsbehörden – die Kompetenz erhalten sollen, beliebige neue Überwachungstypen zu definieren. Darin liegt eine Systemänderung, die den genannten Gewinn an Rechtssicherheit für Bürger und FDA wieder zunichte macht und zudem die Grundsätze des RVOG zur Gesetzesdelegation verletzt.

Und schliesslich führt Art. 24b lit. a Ziff. 4 VÜPF vom Wortlaut her die Speicherung aller verfügbaren Internet-Adressierungselemente ein, zu denen streng genommen selbst IP-Adressen und URLs gehören. Aus IP-Adresse und URL lassen sich aber vielfach auch die abgerufenen Inhalte eruieren. Dies wiederum widerspricht dem Konzept von BÜPF und StPO, gemäss dem nur Randdaten, aber nicht Inhalte für die rückwirkende Überwachung gespeichert werden. Eine Ausdehnung der Überwachung auf IP-Adressen und URLs würde zudem den verfassungsrechtlichen Rahmen der Fernmeldeüberwachung sprengen. Die Bestimmung ist daher insofern eng auszulegen, als nur Adressierungselemente auf der Seite des Teilnehmers, nicht aber solche der jeweils angesprochenen Gegenstelle (IP-Adresse des Webservers oder gar URLs) aufzuzeichnen sind.

Résumé

Il est évident que l'OSCPT, entrée en vigueur en 2001, n'était plus adaptée à notre époque et qu'elle ne pouvait plus vraiment remplir ses fonctions compte tenu des progrès de la technique. Hormis certains aspects marginaux comme la correspondance électronique, l'Ordonnance ne contenait en particulier aucune disposition sur la surveillance d'Internet. Toutefois le service SCPT exigeait une telle surveillance de la part des fournisseurs de services de télécommunication (FST). Les FST ont répondu à cette exigence du moins dans le domaine des réseaux fixes. En revanche les FST se sont élevés avec succès contre l'exigence nouvelle d'une surveillance des liaisons Internet passant par les téléphones mobiles, en faisant valoir que l'Ordonnance n'offrait pas de base légale suffisante. La nouvelle Ordonnance comble cette lacune et contribue ainsi à une plus grande sécurité juridique.

Toutefois, la révision est critiquée, car elle va au-delà de ce qui avait été annoncé, soit une adaptation de l'Ordonnance à la jurisprudence rendue depuis sa mise en vigueur et aux progrès de la technique. Il est regrettable que le Conseil fédéral, compte tenu du caractère politique délicat de la surveillance, soit allé aussi loin et n'ait pas été en mesure d'attendre la révision de la LSCPT, qui était planifiée à

[69] So P. GLOOR, Präsident der SwiNOG Federation.
[70] Vgl. dazu die Hinweise in Fn. 44.

court terme. Il aurait été préférable de laisser décider le législateur, démocratiquement légitimé, plutôt que de s'engager dans une voie critiquable, voire contraire aux règles du droit public.

En outre, ce n'est plus le Conseil fédéral – malgré la jurisprudence récemment rendue par le Tribunal fédéral administratif – mais dorénavant le service SCPT lui-même – et ainsi indirectement les autorités cantonales de répression pénale – qui aura la compétence de définir les nouveaux types de surveillance. Le changement de système anéantit les efforts tendant au renforcement de la sécurité du droit vis-à-vis des citoyens et des FST et ne respecte pas les principes de la LOGA sur la délégation de compétence législative.

Finalement, l'art. 24b let. a ch. 4 OSCPT introduit également l'enregistrement de toutes les ressources d'adressage par Internet auxquelles appartiennent même*, littéralement, les adresses IP et les URL. Mais les contenus téléchargés peuvent souvent être identifiés à partir des adresses IP et des URL, ce qui est contraire à la conception mise en place par la LSCPT et le CPP, selon laquelle seules les données marginales et non les contenus peuvent être enregistrés en vue d'une surveillance rétroactive. Un élargissement de la surveillance aux adresses IP et aux URL sort du cadre constitutionnel de la surveillance des télécommunications. Cette disposition doit donc être interprétée de manière restrictive en ce sens que seules les ressources d'adressage du côté du participant peuvent être enregistrées, et non celles de l'autre partie (adresse IP du serveur ou même les URL).*