Arbeitsgruppe Kommunikationsüberwachung

Arbeitsgruppe Kommunikationsüberwachung (AGKÜ)
Groupe de Travail Surveillance de Communication (GTSC)
Gruppo di Lavoro Sorveglianza della Comunicazioni (GLSC)

Im Auftrag der Konferenz der kantonalen Justiz- und Polizeidirektoren der Schweiz

Informatik Service Center ISC EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Bereich Recht & Controlling
Patrick Schöpf
3003 Bern

Stellungnahme der Arbeitsgruppe Kommunikationsüberwachung (AGKÜ) zur

Teilrevision der Verordnung über die Überwachung des Post-und Fernmeldeverkehrs (VÜPF; SR 780.1) sowie Teilrevision der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (Gebühren-VO; SR 780.115.1;)

1. Ausgangslage

Grundsätzlich ist es zu begrüssen, dass das EJPD endlich eine Teilrevision VÜPF in die Anhörung gibt. Seit 2006 fordert die AGKÜ die Revision der Verordnung VÜPF. Wie jüngste Entscheide des Bundesverwaltungsgerichts belegen, ist eine revidierte Verordnung VÜPF zwingend notwendig, um gegenüber den Fernmeldedienstanbietern (FDA) rechtsgenügende Überwachungsanordnungen zu verfügen und damit das ÜPF die erforderlichen technischen und administrativen Richtlinien erlassen kann. Nur so können FDA verbindlich verpflichtet werden, die gewünschten Daten auszuleiten. Die Verordnung VÜPF hätte ursprünglich mit der BÜPF Revision per 1.1.2011 eingeführt werden sollen. Da sich nun die BÜPF Revision beim Bundesamt für Justiz verzögert und voraussichtlich nicht vor Mitte 2013 in Kraft treten kann, hat sich das EJPD entschieden, eine Teilrevision der Verordnung VÜPF zu machen und nach der BÜPF Einführung 2013 dann eine Totalrevision der VÜPF durchzuführen. Dieses Vorgehen ist etwas unüblich und birgt einige Stolpersteine. So wird nun versucht, in der Teilrevision VÜPF neue Überwachungstypen im Bereich der Internettechnologie zu erfassen. Gleichzeitig wird in der BÜPF Revision darüber diskutiert, wer von den Internetdienstleistern neu unter das Gesetz fallen soll.

Dies hat folgenden Hintergrund. Als das BÜPF im Jahr 2000 erarbeitet wurde, gab es nur gerade die neugegründete Swisscom und den Bereich Telefonüberwachung. Das einzige IT-basierte Produkt war E-Mail, welches zur Überwachung angeboten wurde. Über 90 % der heutigen Überwachungsfälle werden durch die vier grossen Provider Swisscom, Sunrise, Orange und UPC Cablecom durchgeführt. Mit den Bedürfnissen der Strafverfolgungsbehörde, auch die neuen IP basierten Technologien überwachen zu können, öffnet sich der Geltungsbereich plötzlich auf über 600 Internetdienstleister, darunter auch Städte oder Institutionen die öffentliches WLAN anbieten oder Universitäten und Hochschulen etc. Diese würden nach geltendem Recht nun alle verpflichtet, Überwachungstechnik zu installieren und dem Dienst ÜPF die Bereitschaft zu melden, respektive sich zertifizieren zu lassen. Dass dies bei den Fernmeldedienstanbieter und Providern einen grösseren Aufschrei auslöste, ist nachvollziehbar. Deshalb sind im Rahmen der BÜPF Revision auch Anpassungen des Geltungsbereich zu prüfen und neu zu formulieren, welcher Provider oder Fernmeldedienstanbieter welche Verpflichtung hat. Für die AGKÜ ist klar, dass grundsätzlich alle in der Schweiz erbrachten öffentlichen Fernmeldedienstleitungen unter den Geltungsbereich des BÜPF fallen müssen, zum Beispiel auch ausländische Firmen wie Google. Hingegen sieht die AGKÜ nicht ein, weshalb über 600 Provider ständige Überwachungsgeräte installieren sollten, obwohl sie fest davon ausgehen können, gar nie zu einer Überwachung verpflichtet zu werden, sei es weil sie keine Kunden haben oder nur eine Teildienstleistung anbieten oder weiterleiten. Mit der Teilrevision VÜPF greift der Dienst ÜPF dieser BÜPF Diskussion vor und es ist zu befürchten, dass die meisten Provider die Teilrevision VÜPF bekämpfen werden.

Weiter bedauert die die AGKÜ, dass weder sie selbst noch ein Fernmeldedienstanbieter bei der Ausarbeitung der Teilrevision VÜPF beigezogen wurde. Die Teilrevision VÜPF enthält somit nur Revisionspunkte, die der Dienst ÜPF für wichtig hält und auch formuliert hat. Der Dienst ÜPF geht wohl davon aus, dass er die Bedürfnisse und Arbeitstechniken der Strafverfolgungsbehörde so gut kennt, dass er diese als Auftraggeber nicht beiziehen muss. Wir stellen fest, dass der

Dienst ÜPF wenig Bereitschaft zeigt, mit der AGKÜ als Leistungsbezügerin für Fernmeldeüberwachungen zusammenzuarbeiten.

2. Teilrevision VÜPF

Generelles:

Die AGKÜ geht davon aus, dass die Verordnung einerseits den FDA aufzeigen soll, wie der Prozess einer Fernmeldeüberwachung abläuft und welche Überwachungen vorzunehmen sind, respektive welche Resultate die Strafverfolgungsbehörden von den einzelnen Überwachungen erwarten. Anderseits soll sie den Strafverfolgungsbehörden auch aufzeigen, welche Dienstleistungen sie erwarten kann. Um die vorgeschlagenen, neuen Bestimmungen der Teilrevision VÜPF zu verstehen, ist die Lektüre des erläuternden Berichts zwingend, damit man erkennen kann, was Sinn und Zweck der jeweiligen Norm ist. Auf Grund der Differenzen in der Formulierung zwischen dem erläuternden Bericht und der Revisionsvorlage der VÜPF ist davon auszugehen, dass es zu unterschiedlicher Rechtsauslegung kommen kann.

Die AGKÜ spricht sich auch dafür aus, dass in der Verordnung grundsätzlich keine technischen Lösungen beschrieben, sondern die Anforderungen oder die gewünschten Überwachungsresultate vorgegeben werden sollten. Die technischen Lösungen sind in den technischen Richtlinien abzubilden und zwar nach dem Standard des Europäischen Instituts für Telekommunikationsnormen ETSI. Damit wird gewährleistet, dass die FDA Überwachungsgeräte auf dem Europäischen Markt einkaufen können und keine extra helvetische Lösung bauen müssen. Zudem können die technischen Richtlinien einfacher angepasst werden. In der geltenden VÜPF wird in Art. 33 Abs. 1bis nebenbei noch bemerkt, dass der Dienst die Einzelheiten in Richtlinien regelt. Genau diese Einzelheiten bilden aber das Herzstück einer Überwachung. Die AGKÜ schlägt deshalb vor, die Grundzüge der Technischen Richtlinien, was sie beinhalten sollen und wie diese jährlich - unter Mitwirkung von Providern und die Strafverfolgungsbehörden - angepasst werden können, in der VÜPF zu regeln.

Die Struktur der VÜPF beurteilen wir als unübersichtlich und mit Doppelspurigkeiten behaftet. Zudem fehlt eine Konsolidierung mit der einschlägigen Terminologie aus der neuen Schweizerischen StPO und dem Fernmeldegesetz (FMG). So sollten im Sinne der Rechtssicherheit und Einheitlichkeit der Rechtsordnung für die gleichen technischen Gegebenheiten dieselben Begriffe verwendet werden. Die Zersplitterung und Aufgliederung der einzelnen Überwachungstätigkeiten ist unseres Erachtens nicht zielführend. Sie entspricht insbesondere nicht dem Grundsatz der StPO, die generell vom Oberbegriff „Fernmeldeüberwachung" ausgeht und damit die gesamte Fernmeldekommunikation erfasst. Vermutlich könnte die VÜPF entschlackt werden und indem sie nur auf die 3 folgenden Überwachungsgruppen eingeht:

- Echtzeitüberwachung (Kommunikationsüberwachung)
- Rückwirkende Überwachung (Verkehrsdatenerhebung)
- Technische Auskünfte (Teilnehmeridentifikation)

Mit welchem Fernmeldeangeboten die zu überwachende Kommunikation erfolgt, ist für die Anordnung der Kommunikationsüberwachung nicht relevant und kann zu Komplikationen führen, wenn der datenlieferungspflichtige Provider der Meinung ist, dass eine bestimmte Fernmeldekommunikationsform durch die Anordnung nicht erfasst sei. Vielmehr muss im Grundsatz vorab eine generelle Anordnung der Fernmeldeüberwachung erfolgen.

Zu den einzelnen Bestimmungen der Revisionsvorlage

Obschon einige der nachstehend erwähnten Normen nicht Gegenstand der Teilrevision bilden sollen, erscheint es uns sachdienlich, zusätzliche Verbesserungsvorschläge zu formulieren, damit die Zusammenarbeit mit dem Dienst ÜPF für die tägliche Praxis verbessert werden kann.

Zu Art. 1 VÜPF

In der Praxis erweist es sich oft als problematisch, dass die auswertende Behörde, in der Regel die Polizei, keine Anordnungskompetenzen gegenüber dem ÜPF hat. Grundsätzlich korrespondiert der ÜPF nur mit der anordnenden Behörde, also der Staatsanwaltschaft. Auch wenn am Grundsatz der Gesamtverantwortung der Staatsanwaltschaften nichts geändert werden soll, wäre es für eine reibungslose Abwicklung der Überwachungsaufträge dienlich, wenn auch die auswertende Behörde dem ÜPF im Auftrag des Staatsanwalts Vorgehensanweisungen erteilen kann, ohne dass die Staatsanwaltschaft hierfür zusätzliche Verfügungen erlassen muss. Dies betrifft zum Beispiel die Anweisung, auswertende Personen bei den Überwachungsmassnahmen aufzuschalten.

Die AGKÜ schlägt deshalb vor, in Art. 1 Abs. 2 lit. b die auswertende Behörde zusätzlich zu erwähnen.

Zu Art. 2 VÜPF

Die AGKÜ schlägt vor, die Definitionen der Fernmeldegesetzgebung zu übernehmen, damit die gleiche und Terminologie einheitlich verwendet wird.

Art. 3 VÜPF

Wir schlagen die Aufnahme eines zusätzlichen Abs. 3 vor:

3 *Der Dienst unterstützt Strafverfolgungsbehörden und Fernmeldedienstanbieter bei der rechtskonformen und zweckmässigen Datenlieferung bei Fernmeldeüberwachung.*

Art. 3 sollte verstärkt die Funktion des ÜPF zum Ausdruck bringen. Dieser ist in erster Linie ein Dienstleister, welche die Datenübermittlung der FDA an die Strafverfolgungsbehörden vornimmt. Im Rahmen der Beweiserhebung können dem ÜPF auch keine Entscheidbefugnisse zukommen, zumal die StPO die Leitung des Vorverfahrens allein der Staatsanwaltschaft und die Genehmigung der Überwachungen dem Zwangsmassnahmengericht zuweist. Es wäre wünschenswert, wenn er einvernehmlich mit den Strafverfolgungsbehörden und den Fernmeldedienstanbieterin zusammen arbeiten würde und diese Zusammenarbeit auch in einem verbindlichen Geschäftsreglement geregelt wäre.

Art. 4 VÜPF

Hier wäre im Sinne der Bemerkungen zu Art. 1 vorstehend zu ergänzen:

a. der Behörden, die zur Anordnung ***und Auswertung*** einer Überwachung zuständig sind;.

Zu Art. 5 Abs. 1 lit. a VÜPF

Wir schlagen vor, die Bestimmung wie folgt zu ergänzen:

"... mit einem anderen durch das Departement zugelassenen sicheren Übertragungsmittel, ***insbesondere durch elektronische Vorerfassung im Überwachungssystem.***"

Aus praktischer Sicht wäre es vorteilhaft, auf die vielen technischen Formulare verzichten zu können. Stattdessen sollten Polizei oder Staatsanwaltschaft die Massnahme direkt selbst im Überwachungssystem vorerfassen und einrichten können. So könnte der Dienst ÜPF die Massnahme umgehend freischalten, sobald ihm die Überwachungsanordnung vorliegt. Mit der vorgeschlagenen Ergänzung wäre sichergestellt, dass eine rechtlich zulässige elektronische Schnittstelle bestehen kann. Zudem garantiert eine elektronische Informationsübermittlung die Vollständigkeit der übermittelten Daten und bildet somit - neben dem unbestreitbaren Effizienzgewinn - ein Element der Datensicherheit und der Nachvollziehbarkeit. So würde auch der seit 2006 geforderten Prozessoptimierung Rechnung getragen. Damals wurde im Kontext der Gebührenfestlegung seitens Bund und KKJPD festgestellt, dass die hohen Gebühren vor allem durch die zahlreichen Medienbrüche bei der Bestellung der Überwachung verursacht werden.

Art. 7 VÜPF

Mit Blick auf unseren Vorschlag zu Art. 1 ist die Bestimmung wie folgt zu ergänzen:

1 Die Behörden, die Überwachungen anordnen, ***auswerten*** oder genehmigen, sowie die Anbieterinnen von Post- oder Fernmeldediensten können diejenigen Personendaten bearbeiten, die sie für die Kontrolle der Ausführung der Überwachungsanordnungen benötigen.

Art. 8 Abs. 1*:*

Um zum Ausdruck zu bringen, dass die Kommunikationsüberwachung einer effizienten und effektiven Strafverfolgung zu dienen hat, schlagen wir folgende Ergänzungen der Bestimmung vor:

1 Der Dienst errichtet und betreibt ***ein auf die Bedürfnisse der Strafverfolgungsbehörden ausgerichtetes*** Verarbeitungszentrum für die Daten aus der Überwachung des Fernmeldeverkehrs und der Kommunikation im Internet.

zu Abs. 2

a. "... der Überwachung des Fernmeldeverkehrs ***gemäss den technischen Richtlinien*** entgegenzunehmen ..."

Hierzu ist auf die Darlegung der Ausgangslage zu verweisen. Die beschleunigte Technologieentwicklung erfordert, dass flexibler auf Neuerungen reagiert werden kann, ohne die Verordnung jedesmal anpassen zu müssen. Die technischen Richtlinien können ohne grossen administrativen Aufwand an neue, noch nicht absehbare technische Entwicklungen angepasst werden. Mit einem solchen Verweis auf die technischen Richtlinien können technische Veränderungen aufgefangen werden.

b. "... für die betroffene Strafverfolgungsbehörde bereitzustellen, **diese mittels eines online-Abrufverfahrens zugänglich zu machen oder elektronisch zu übermitteln**."

Mit der vorgeschlagenen Ergänzung würde die bereits seit langem geforderte Schnittstelle zum System JANUS ermöglicht. JANUS ist ein schweizweites polizeiliches Informationssystem, in welchem unter anderem Fernmeldeüberwachungsdaten ausgewertet, bewertet und für das Verfahren komplettiert werden.

Art. 9 Abs. 2:

Wir schlagen vor, die Bestimmung wie folgt zu ergänzen:

2 Die Anbieterinnen von Post- oder Fernmeldediensten folgen den Anweisungen des Dienstes für die Datensicherheit bezüglich der Übertragung der Überwachungsdaten. Sie sind für die Datensicherheit bis zum Übergabepunkt der Daten an den Dienst verantwortlich. ***Der technische Übergabepunkt ist so nahe wie möglich beim Verarbeitungszentrum des Dienstes ÜPF.***

Mit Blick auf die gesetzliche Lieferungspflicht der FDA ist eine aus Sicht der Leistungsbezüger günstige Definition des örtlichen Übergabepunktes anzustreben. Offenbar prüft der ÜPF derzeit gestützt auf neue Technologien, die Daten auf der Strecke zum Provider abzuholen. Dies würde Mehrkosten im Delivery Netzwerk auslösen, die letztlich auch von den Strafverfolgungsbehörden über entsprechend erhöhte Gebühren zu tragen wären.

Zu Art. 10 Abs. 1 VÜPF

Aus unserer Sicht muss die Bestimmung wie folgt neu gefasst werden:

1 Der Dienst vernichtet die Daten gestützt auf einen Vernichtungsauftrag der Anordnungsbehörde. Bis zu diesem Zeitpunkt bewahrt der Dienst die Daten sicher auf.

Der Vorschlag für diese Neuformulierung stützt sich auf zwei Überlegungen. Um der Gefahr eines versehentlichen Datenverlusts entgegenzutreten, soll die Vernichtung nur gestützt auf eine entsprechende Anordnung des Auftraggebers für die Überwachung veranlasst werden. Andererseits soll damit die Archivierung der Daten an einem einzigen Ort möglich sein, mindestens bis zum Zeitpunkt, an dem die Daten gesichert und justiziabel in den Aktenbestand des Strafverfahrens eingefügt sind.

Zu Art. 10 Abs. 2 VÜPF

Diese Bestimmung ist entsprechend anzupassen:

Er vernichtet die Daten aus der Geschäftskontrolle ein Jahr ***nach der Vernichtung der Datengemäss Abs. 1***.

Es ist folgerichtig, dass die Auffindbarkeit in der Geschäftskontrolle mindestens so lange erhalten bleiben muss, bis auch keine entsprechenden Daten mehr vorhanden sind. Die Geschäftskontrolle muss Auskunft darüber geben können, welche Daten wo noch vorhanden sind. Aus Gründen der Kontrollierbarkeit soll denn auch hier die Geschäftskontrolle noch mindestens 1 Jahr nach Vernichtung der Daten diesen Geschäftsvorgang ausweisen können.

Die Abschnitte 4. - 6. der vorgeschlagenen Teilrevision VÜPF sind nach Meinung der AGKÜ nochmals zu überarbeiten und zu straffen. Es genügt, den Vorgang der Bestellung einer Fernmeldeüberwachung oder die Auf- und Abschaltung einer Massnahme einmal zu erklären, denn er ist für Telefonie wie auch für das Internet identisch. Dabei ist auch verstärkt auf die tatsächlichen Abläufe bei den Strafverfolgungsbehörden Rücksicht zu nehmen. Diese bestellen nämlich die Fernmeldeüberwachung mit Bezug auf bestimmte Personen und nicht auf einen speziellen Dienst oder ein Adressierungselement. Das Adressierungselement hilft nur, den Anschluss zu identifizieren, mehr nicht. Dabei entscheidet wie eingangs erwähnt die Strafverfolgungsbehörde selbst, ob sie eine Echtzeitüberwachung des Fernmeldeverkehrs, die Einholung der Verkehrsdaten oder von technischen Auskünften, worunter eigentlich auch die Beauskunftung der Adressierungselemente fallen, wünscht.

Bei einer Mobilfunküberwachung fordert die Strafverfolgungsbehörde alle Fernmeldedaten, die über das Mobilfunkgerät empfangen oder gesendet werden ein und zwar gemäss den techni-

schen Richtlinien nach ETSI. Sie wird bei einer Mobilfunküberwachung kaum je nur die Telefonkommunikation mit SMS aber ohne MMS bestellen.

Das gleiche gilt bei der Überwachung des Internetverkehrs einer Festnetznummer. Da kann die Strafverfolgungsbehörde auch nicht nur den "Facebook-Datenverkehr" bestellen, sondern erhält den ganzen ein- und ausgehenden Internetverkehr geliefert.

Bei der Echtzeitüberwachung unterscheidet die Strafverfolgungsbehörde zwischen den Hauptkategorien Festnetz oder Mobilfunk, wobei Telefon oder IP Daten oder Kopfschaltung etc. eingeschlossen sind und als eine Massnahme gelten.

Bei den Verkehrsdaten verlangt die Strafverfolgungsbehörde die durch ETSI erarbeiteten Richtlinien "Data Retention" die Verkehrsdaten der einzelnen Überwachungsservices.

Bei den technischen und administrativen Auskünften muss die Strafverfolgungsbehörde mittels elektronischen automatisiertem Auskunftssystem (CCIS) alle Adressierungselemente oder Personen rund um die Uhr Abfragen können.

Die richtige Beschreibung der drei Hauptkategorien Echtzeitüberwachung, Verkehrsdatenerhebung oder technische administrative Auskünfte würden also vollends genügen.

Dass man mit Blick auf die Leistungspflicht der FDA auch Überwachungstypen aufzählt, ist letztlich überflüssig, da diese in den technischen Richtlinien ausführlich beschrieben werden. Es genügt, wenn die Verordnung die Grundverpflichtung der FDA klar wiedergibt. Die technischen Richtlinien, die als Anhang zur Verordnung gehören, beschreiben im Detail, welche Überwachungstypen wie ausgeführt werden müssen. In der Verordnung könnte daher lediglich aufgenommen werden: *Als Überwachungstypen im Sinne von Art. 270 ff StPO gelten namentlich: die Überwachung des Fernmeldeverkehrs im Festnetz und im Mobilfunk.*

Zu Art. 24a Abs. d lit 4. VÜPF

4. bei der Überwachung von E-Mail-Verkehr: Die Umschlaginformationen.

...gemäss SMTP-Protokoll ist zu streichen. Es existieren heute bereits andere Protokolle (IMAP, POP3), die so nicht abgedeckt wären. In Zukunft könnte es andere Protokolle geben, die dann wiederum nicht abgedeckt wären. Dieser Passus gehört nicht in die VÜPF, sondern muss in den technischen Richtlinien geregelt werden.

Zu Art. 24b Abs. b lit 2. VÜPF

4. bei der Überwachung von E-Mail-Verkehr: Die Umschlaginformationen.

...gemäss SMTP-Protokoll ist aus den gleichen Gründen wie vorstehend zu streichen.

3. Teilrevision der Gebührenverordnung

Wir sind der Auffassung, dass die die Kosten einer PS 1 Überwachung in der Gebührenverordnung bekämpft werden müssen. Ungeachtet der Erklärung des ÜPF für diese Kosten, sind diese für die AGKÜ nicht nachvollziehbar.

Eine einfache Mobilfunküberwachung, also zum Beispiel die Abhörung von Gesprächen, SMS und MMS wird neu Kosten von CHF 8570.00 generieren. Darin enthalten ist eine Schaltung Telefonie (CS1-3) für CHF 2410.-- und eine Schaltung Mobil IP (PS1) für CHF 6160.--.

Handelt es sich bei obgenannter Mobilfunküberwachung um ein ausländisches Adressierungselement, was ja bei einer Rechtshilfe der Fall ist, oder will man zusätzlich auch die IMEI Nummer schalten lassen, ist man gezwungen, diese Überwachung bei allen Fernmeldeprovidern schalten zu lassen, was für die Strafverfolgungsbehörde bedeutet, dass eine solche Überwachung eine Kostenexplosion von CHF 25'710.00 zur Folge hätte. Dies erscheint auch deshalb nicht gerechtfertigt, weil man bei einem Verbindungsaufbau nur Daten von einem Provider und nicht von allen, die für die Überwachung Geld bekommen, erhält.

Die Berechnung des Speicherbedarfs bezieht sich auf eine Festenetzüberwachung mit einem durchschnittlichen Datenzuwachs von 20 GByte pro Monat. Dies ist für eine Mobilfunkinternetüberwachung unrealistisch. Gängige „Flat Rate“ Angebote der FDA limitieren den maximal möglichen Datenbezug auf 100 MByte pro Monat. Dies ist 200-mal weniger als im Rechenbeispiel. Ausserdem ist zu bedenken, dass bei einer IMEI Schaltung der Dienst das Dreifache an Gebühren einnimmt, obwohl er nur eine Massnahme schaltet.

Wir schlagen vor, eine technische Analyse und Prozessüberprüfung, insbesondere in Bezug auf das neue ISS, durchzuführen, die eine objektive Bewertung zulassen und Grundlagen für die Kostenberechnung liefern. Wie bereits die 2006 durchgeführte Prozess- und Kostenüberprüfung der Firma TC Team Consult, damals im Auftrag des UVEK und der KKJPD, aufzeigte, entstehen dem Provider für die Schaltung einer Echtzeitüberwachung einer Rufnummer Kosten von maximal CHF 150.--. Er wird gemäss Gebührenverordnung vom Dienst ÜPF dafür aber mit CHF 1330.— entschädigt und der ÜPF verlang von den Strafverfolgungsbehörde für seine Dienstleistung CHF 2410.--. Schon dieses Beispiel und die Grundlagen des genannten Berichtes zeigen, dass der Dienst ÜPF die Gebühren für die Überwachungen längst senken und nicht erhöhen müsste. Wenn unsere Überwachungskosten gesenkt werden, wären sie mit denjenigen in Deutschland vergleichbar, wo eine Echtzeitüberwachung einer Rufnummer ca. 100 Euro kostet.

Der Dienst ÜPF begründet seine hohen Gebühren auch mit seinem niedrigen Kostendeckungsgrad, den der ÜPF hat. Die AGKÜ beurteilt das Preis-Leistungsverhältnis für die Dienstleistungen

des ÜPF schon länger kritisch. Der Dienst ÜPF hat sich personell zwar stark vergrössert, aber die Synergiegewinne durch die Verschiebung des ÜPF vom UVEK in das EJPD sind ausgeblieben. Insbesondere der harzige Verlauf des Beschaffungsprojekt ISS, das stark im Verzug ist , aber auch die Schwierigkeiten im Zusammenhang mit Internetüberwachungen zeigen, dass der ÜPF auch mit mehr Personal nicht in der Lage ist, für die Strafverfolgungsbehörden bedürfnisgerechte, kostengünstige und effiziente Dienstleistungen anzubieten. Störend ist auch, dass der ÜPF seinen Kostendeckungsgrad offenbar zu Lasten der Strafverfolgungsbehörden optimieren will, im Gegenzug aber nicht bereit ist, die Kantone und den Bund als Hauptleistungsbezüger angemessen in die Zusammenarbeit einzubeziehen. Trotz entsprechender Bemühungen seitens der Strafverfolgungsbehörden der Kantone und des Bundes ist eine Regelung für eine Zusammenarbeit auf Augenhöhe bislang nicht zustande gekommen.

PS2, PS3, PS4

Diese Überwachungstypen sind in den ETSI Standards nicht vorgesehen. Im Gegensatz zur konventionellen Telefonie, kann im Internet technisch nicht zwischen Nutz- und Verkehrdaten unterschieden werden. Würden diese Typen eingeführt, sind schweizspezifische, kostenintensive Anpassungen an den Überwachungsanlagen der FDA notwendig. Eine solche Entwicklung ist zu vermeiden.

A 0.1 / A0.2

Es ist technisch nicht nachzuvollziehen, wieso die Abklärung einer statischen IP Adresse mit Fr. 10.- abzugelten ist, die Abklärung einer dynamischen hingegen mit Fr. 250.--. Bei den FDA wird dasselbe Equipment eingesetzt. Die Auskunft sollte deshalb generell mit Fr. 10.-- abgegolten werden. Dies ist immer noch 2,5-mal mehr als die Auskunft bei den CS A0 mit Fr. 4.--

Zürich und Bern, 5.7.2011

Für die AGKÜ

Gez.	Gez.	Gez.
Beni Weder Leiter AGKÜ	Felix Ceccato stv. Leiter AGKÜ	Walter Irminger Leiter Study Group ISS AGKÜ

Schweizerischer Verband der Telekommunikation
Association Suisse des Télécommunications
Swiss Telecommunications Association

Einschreiben
Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und
Fernmeldeverkehr
Bereich Recht und Controlling
Herr Patrick Schöpf
3003 Bern

Bern, 29. Juli 2011

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

Sehr geehrter Herr Schöpf

asut wurde mit Mail vom 8. Juni 2011 eingeladen, 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 bis zum 29. Juli 2011 Stellung zu beziehen. Wir bedanken uns für die Einladung zur Stellungnahme und nehmen diese hiermit fristgerecht wahr.

Die asut-Stellungnahme setzt sich aus folgenden Dokumenten zusammen:

- Stellungnahme asut VÜPF
- Stellungnahme asut VÜPF – Technischer Anhang

Wir danken Ihnen für die Berücksichtigung der Interessen der Telekommunikationsbranche.

Freundliche Grüsse

asut – Schweizerischer Verband
der Telekommunikation

Dr. Fulvio Caccia
Präsident asut

Klösterlistutz 8 / 3013 Bern
T: +41 31 560 66 66 / F: +41 31 560 66 67 / info@asut.ch / www.asut.ch

Schweizerischer Verband der Telekommunikation
Association Suisse des Télécommunications
Swiss Telecommunications Association

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

Management Summary

Mit Schreiben vom 8. Juni 2011 eröffnete Bundesrätin Simonetta Sommaruga eine 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. Mit dem vorliegenden Papier nimmt der schweizerische Verband der Telekommunikation asut zu den vorgeschlagenen Änderungen kritisch Stellung.

Die folgenden Punkte stehen dabei im Zentrum:

1. Entgegen der Darstellung im Begleitbrief würde die vorgeschlagene Revision nicht nur eine Nachführung der bereits bestehenden Praxis darstellen, sondern eine **massive Ausweitung der staatlichen Überwachung** des Bürgers mit sich bringen, insbesondere eine Vorratsdatenspeicherung des Internetverkehrs. Es handelt sich um einen eigentlichen **Etikettenschwindel,** der im geltenden Bundesgesetz über die Überwachung des Post und Fernmeldeverkehrs BÜPF zudem gar **keine genügende gesetzliche Grundlage** findet und kaum auf statistischen Entscheidgrundlagen basiert.
2. Sodann bringt die Vorlage, anders als in den Erläuterungen dargestellt, **keine Verbesserung der Rechtssicherheit.** Entgegen der Regelung in der geltenden VÜPF soll nämlich der Katalog der Überwachungspflichten in der neuen VÜPF nicht mehr abschliessend sein, sondern die Behörden sollen explizit auch die Kompetenz erhalten, ohne Verordnungsgrundlage neue Überwachungspflichten einzuführen. Anders als unter der geltenden Verordnung haben die Telekom-Unternehmen wie auch die Bürger damit genau *keine* Rechtssicherheit mehr; sie werden nicht mehr wissen, mit welchen Überwachungsmassnahmen sie zu rechnen haben.
3. Die Vorlage soll für die Behörden eine **Kostensenkung** bringen, diese würde allerdings genau besehen **ausschliesslich zu Lasten der Telekom-Unternehmen** gehen. Schon heute werden die Kosten der Telekom-Unternehmen für die Kommunikationsüberwachung nur zu einem Drittel vom Staat entschädigt. Die asut kann nicht nachvollziehen, warum dieser Betrag jetzt auf dem Buckel der Telekom-Unternehmen und ihrer Kunden noch weiter gesenkt werden soll. Mit der Kostensenkung für die Behörden droht den Telekom-Unternehmen zudem eine massive Steigerung der Zahl von Überwachungsaufträgen, für die sie dann wiederum die Mehrheit der Kosten zu tragen hätten.
4. Die Vorlage **ignoriert das Verhältnismässigkeitsprinzip**: Die Telekom-Unternehmen sollen nicht verpflichtet werden können, teure Überwachungsanlagen zu beschaffen, die sie ohnehin nur in sehr unwahrscheinlichen Fällen überhaupt brauchen werden.

Aus diesen Gründen steht die asut der aktuellen Revision der VÜPF ablehnend gegenüber. Vor allem die geplante Ausweitung der Überwachungsmassnahmen darf nur mit einem demokratisch legitimierten Entscheid und damit nur durch Bundesgesetz erfolgen. **Entsprechend ist mit einer Revision der VÜPF bis zur Verabschiedung des BÜPF zuzuwarten.**

Der asut geht es mit ihrer Opposition gegen die Vorlage keineswegs darum, den Sinn der Telekom-Überwachung zum Zweck der Verbrechensbekämpfung in Frage zu stellen. **Die asut und ihre Mitglieder haben vielmehr schon immer konstruktiv mit den Behörden zusammengearbeitet, um die gesetzlich vorgesehenen Überwachungsmassnahmen umzusetzen.** Die asut wehrt sich allerdings gegen die neuesten Reformpläne, weil derart schwerwiegende Eingriffe in die Privatsphäre des Bürgers und in die Wirtschaftsfreiheit und Eigentumsgarantie der Telekom-Unternehmen nicht durch die Hintertür einer Verordnungsrevision eingeführt werden dürfen.

Klösterlistutz 8 / 3013 Bern
T: +41 31 560 66 66 / F: +41 31 560 66 67 / info@asut.ch / www.asut.ch

1 Allgemein

1.1 Teilrevision?

Gemäss dem Begleitbrief vom 8. Juni 2011 zur Vorlage, unterzeichnet durch Frau Bundesrätin Simonetta Sommaruga, soll es bei vorliegender Teilrevision der VÜPF lediglich um eine „Nachführung“ gehen, welche für alle Beteiligten „die nötige Bestimmtheit und Rechtssicherheit“ schaffe. Dies trifft jedoch nicht zu:

- Zunächst wird mit der Vorlage keineswegs nur die bestehende Praxis nachgeführt, sondern es werden auch diverse neue Überwachungsmassnahmen verankert, wie z.B. eine umfassende Überwachung des Internetverkehrs, zudem sollen internationale Kopfschaltungen analog zur Sprachtelefonie neu auch für SMS- und Internetüberwachungen gemacht werden. Bisher wurden als Folge eines Entscheids des Bundesverwaltungsgerichts internationale Kopfschaltungen lediglich hinsichtlich der Gesprächstelefonie eingesetzt.

- Sodann sollen mit der Revision nicht nur zweifelhafte Massnahmen wie die Kopfschaltungen in den Katalog aufgenommen werden, sondern neu auch eine Massnahme, welche unseres Erachtens illegal ist, nämlich die Antennensuchläufe. Bei solchen Massnahmen existieren keine Verdachtsmomente gegen bestimmte Personen oder Anschlüsse, wie dies von StPO und BÜPF eindeutig gefordert würde, sondern es wird ein Gebiet unspezifisch nach strafrechtlich Verwertbarem abgesucht.

- In den Erläuterungen wird zudem dargelegt, die Revision senke die Kosten: Aus Sicht der Überwachungsbehörden mag dies zwar zutreffen. Denn dadurch dass gewisse nicht vorgesehene Massnahmen in der Verordnung neu typisiert würden, gäbe es für deren Umsetzung für die Fernmeldediensteanbieter (FDA) nur noch eine geringe Pauschalentschädigung gemäss Gebührenverordnung und keine Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung mehr. Eine solche „Kostensenkung“ erfolgt aber auf dem Buckel der FDA und entspricht, zumindest nach offizieller Lesart, nicht die Meinung der Revision.

- Weiter ist der verwendete Begriff „Teilrevision“ irreführend. Gemäss den Erläuterungen handelt es sich offenbar nur dann um eine Totalrevision der VÜPF, wenn sie im Nachgang einer BÜPF-Revision geschieht. Vom materiellen Gehalt her haben wir es aber bereits vorliegend mit einer Totalrevision der VÜPF zu tun, welche Entscheidungen vorwegnehmen soll, welche eigentlich in den Rahmen der BÜPF-Revision gehören.

1.2 Kein Plus an Rechtssicherheit

Die Vorlage bringt kein Plus an Rechtssicherheit, wie dies in Begleitbrief und Erläuterungen behauptet wird.

Die neueste Praxis des Bundesverwaltungsgerichts vom 21. resp. 23. Juni 2011 bestätigte die Auffassung zweier Mitglieder der asut, dass der Katalog der in der VÜPF geregelten Überwachungsarten abschliessend sei. Art. 17 Abs. 5 und Art. 25 Abs. 5 des Revisionsentwurfs widersprechen diesem Anspruch an die Rechtssicherheit im Sinne der Vorhersehbarkeit, indem sie explizit eine Kompetenz des Dienstes zur Überwachung des Post- und Fernmeldeverkehrs ÜPF zur Einführung weiterer Überwachungsmassnahmen vorsehen.

Aber selbst dann, wenn man der Auffassung ist, der Katalog sei entgegen der Auffassung des Bundesverwaltungsgerichts nicht abschliessend, bringt eine offene Formulierung des Katalogs nichts, da Fernmeldedienstanbieter und Bürger jederzeit damit rechnen müssen, dass entweder die Praxis den Katalog nicht als abschliessend betrachtet oder dass bei Bedarf einfach der Katalog wieder beliebig erweitert wird.

Dass die FDA überdies kein Rechtsmittel besitzen, um sich gegen solche von Gesetz und Verordnung nicht gedeckten Überwachungsmassnahmen zu wehren und ihre verfassungsmässigen Rechte zu wahren, hat die asut bereits in der Vernehmlassung zum VE-BÜPF heftig kritisiert. Sie sieht darin einen wesentlichen konzeptionellen Mangel des BÜPF, der weder durch den VE-BÜPF, geschweige denn durch die nun geplante Verordnungsrevision behoben wird.

Die Erklärung, dass den rechtsstaatlichen Mängeln des BÜPF mit einer VÜPF-Revision nicht beizukommen ist, findet sich im Prinzip in den Erläuterungen zur Vorlage selbst, S. 1 unten:

Nach Ansicht der anordnenden Strafverfolgungsbehörden und der die Überwachungsmassnahmen genehmigenden Zwangsmassnahmengerichte ist die Liste der Überwachungsmassnahmen in der VÜPF nicht abschliessend zu betrachten. Der Dienst und die FDA sind nach dieser Auffassung daher auch

verpflichtet, angeordnete und genehmigte Überwachungsmassnahmen durchzuführen, die nicht explizit in der VÜPF aufgeführt sind. Diese Situation führt zu einer grossen Rechtsunsicherheit und dazu, dass sowohl auf Seiten des Dienstes als auch auf Seiten der FDA bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmassnahmen erhebliche Kosten entstehen.

Die Problematik, dass aufgrund fehlender Rechtsbehelfe der Provider theoretisch alles durchgeführt werden muss, was Zwangsmassnahmengerichte, welche über kein genügendes technisches Verständnis verfügen, genehmigen, lässt sich mit einer Erweiterung des Massnahmenkatalogs sicher nicht beseitigen, solange dieser derart offen formuliert bleibt.

Damit würde nur erreicht, dass damit insgesamt den FDA die Entschädigungen gekürzt würden, weil die Aufwandsentschädigung gemäss bisherigem Art. 4 der Gebührenverordnung durch pauschal festgelegte Teilentschädigungen ersetzt würde. Weiter würde der neue Art. 1 Abs. 2 bis bewirken, dass pro überwachte Rufnummer unter einem Auftrag sämtliche möglichen Erhebungen verlangt werden könnten und dies nur unter Entschädigung der Basisleistung. Die FDA lehnen dies selbstverständlich ab. Es ist in den Erläuterungen nirgends die Rede davon, dass eine Kürzung der Entschädigungen für die FDA die Absicht wäre. In finanzieller Hinsicht ist in den Erläuterungen auf S. 2 vielmehr die Rede davon, dass es darum gehe, den FDA Investitionssicherheit zu verschaffen.

1.3 Übernahme von bisheriger Rechtssprechung und Praxis:

Oft soll mit Gesetzesrevisionen die in der Zwischenzeit aufgelaufene, „bewährte“ Rechtssprechung ins neue Gesetz einfliessen, so auch hier. In diesem Fall ist aber Skepsis angebracht. Einerseits gibt es keine gefestigte Rechtssprechung, sondern nur einige wenige Einzelentscheide, und diese sind meistens nicht hilfreich. Aufgrund der konzeptionellen Fehler im BÜPF, welche zur Folge haben, dass hinsichtlich der Frage, was die Gerichte auf Beschwerde einer FDA hin nun zu prüfen haben, Konfusion herrscht, konnte sich keine Gerichtspraxis entwickeln, welche sich eignen würde, ins Gesetz aufgenommen zu werden.

An dieser Stelle kann nicht auf die Gesamtheit der Unstimmigkeiten und Widersprüchlichkeiten der aufgelaufenen Gerichtsentscheide eingegangen werden, nur soviel: Mit seinen zwei neusten Entscheiden hiess das Bundesverwaltungsgericht zwei Beschwerden von FDA gut, mit der Begründung, die FDA seien in der angefochtenen Verfügung zu Überwachungsmassnahmen verpflichtet worden, welche im Katalog der Überwachungsmassnahmen gemäss VÜPF gar nicht vorhanden sind. Da die Aufzählung der Überwachungsmassnahmen in der VÜPF abschliessend zu verstehen sei, sei eine Verpflichtung der FDA zu Massnahmen ausserhalb des Katalogs nicht zulässig. Gemäss Art. 13 Abs. 1 Bst. a BÜPF darf jedoch der ÜPF eine von Zwangsmassnahmengerichten genehmigte Überwachung nur darauf hin überprüfen, ob die angeordnete Massnahme von einer zuständigen Behörde aus erfolgt ist und ob es um ein Delikt gemäss des Deliktskatalogs des BÜPF geht. Das BVGer hat nun aber darüber hinaus geprüft, ob die angeordneten Massnahmen im Katalog der VÜPF aufgeführt seien. Den FDA ist es zwar durchaus recht, wenn das Bundesverwaltungsgericht in Ausübung einer rechtspolitischen Lückenfüllung über Art. 13. Abs. 1 Bst. a BÜPF hinaus prüft. Es erscheint aber unschlüssig, wenn sich das Gericht einerseits nicht an Art. 13 Abs. 1 Bst. a BÜPF hält und andererseits die von der Beschwerdeführerin angeführten, in diesem Papier auch schon erwähnten, konzeptionellen Fehler des BÜPF in Abrede stellt (A-8267/2010, Erw. 3.2).

Mit dem einzigen höchstrichterlichen Entscheid im Bereich Zulässigkeit von Überwachungsmassnahmen im Fernmeldebereich (BGE 130 II 249ff) wurde überdies eine Überwachungsmassnahme, welche ebenfalls nicht dem VÜPF Katalog angehört (Antennensuchläufe), nicht verhindert. Das Bundesgericht stellte sich dabei auf den Standpunkt, es dürfe die Rechtmässigkeit von Antennensuchläufen gar nicht prüfen. Wenn also in den Erläuterungen behauptet wird, Antennensuchläufe seien von der Gerichtspraxis als zulässig bestätigt worden, so stimmt das schlicht nicht, denn das Bundesgericht hat die Zulässigkeit von Antennensuchläufen gar keiner Prüfung unterzogen. Es wäre daher nicht gerechtfertigt, den Überwachungstypenkatalog der VÜPF unter Hinweis auf die Bundesgerichtspraxis zu ergänzen.

1.4 VÜPF-Revision im jetzigen Zeitpunkt ist abzulehnen

Aus den diversen oben genannten Gründen, ist diese VÜPF-Teilrevision abzulehnen. Wie dargelegt, ist es nicht möglich, mit dieser Vorlage Rechtssicherheit zu schaffen. Es besteht hingegen die Befürchtung, dass mit dieser VÜPF-Revision im etwas kleineren Kreis und ohne die nötige demokratische Legitimation Forderungen durchgedrückt werden sollen, welche in einer Revision des Gesetzes im formellen Sinn keine Chance hätten. Weiter muss die Befürchtung bestehen, dass mit dieser Verordnungsrevision, welche im Prinzip eine Wunschliste des ÜPF enthält, die längst fällige BÜPF-Revision auf die lange Bank geschoben werden soll.

1.5 BÜPF-Revision abwarten

Die meisten relevanten Änderungen in dieser VÜPF-Revisionsvorlage betreffen Punkte, welche gerade in der parallel laufenden BÜPF-Revision umstritten sind:

- Änderungen, welche die Kosten/Entschädigungen betreffen
- Nicht nur Ausleitung des gesamten Fernmeldeverkehrs von bestimmten Breitbandanschlüssen, sondern auch Überwachungspflichten der Zugangsanbieterinnen auf der Dienste-/Anwendungsebene (allfällige Filterungspflichten der FDA)
- Überwachungsmassnahmen gegen einen unbestimmten Personenkreis (z.B. Antennensuchläufe).

Man kann sich daher des Eindrucks nicht erwehren, der Verordnungsgeber wolle nun die Punkte, die im Rahmen der Vernehmlassung zum BÜPF ins Schussfeld der Kritik geraten sind, am Gesetzgeber vorbei in die VÜPF bringen. Damit würde der von Verfassung und Gesetz vorgesehene Stufenbau (Gesetz – Verordnung – Richtlinien) umgangen, was dem Prinzip der Rechtsstaatlichkeit widerspricht. Es geht nicht an, dass die relevanten Entscheidungen auf einer unteren Normenstufe gefällt werden und sich dann später das Gesetz im formellen Sinn danach richten soll.

Dies gilt insbesondere auch deshalb, weil der Verordnungsgeber die ihm durch Art. 15 (insbes. Abs. 6) BÜPF verliehene Rechtsetzungskompetenz in verschiedener Hinsicht eindeutig überschreitet: So regelt das BÜPF beispielsweise an keiner Stelle die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste, die nicht von Fernmeldediensteanbietern oder Internet-Access-Providern, sondern von Internet-Anwendungsanbietern (Service Provider) angeboten werden (vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch hatte der historische Gesetzgeber vor elf Jahren keine Vorstellung, welche neuen Dienstleistungen auf dem Internet zur Verfügung stehen würden, und entsprechend ist der Verordnungsgeber erst durch ein formelles Gesetz zu ermächtigen, Überwachungsarten einzuführen, die zum Zeitpunkt des Erlasses des BÜPF nicht vorstellbar waren (etwa Zugänge über VPN oder „Instant Messaging“). Dies gilt erst recht für eine Vorratsdatenspeicherung für WWW-Internetverkehr (http), die bei einer weiten Auslegung der Verordnung ebenfalls möglich wäre, und die einen schwerwiegenden Eingriff in die Privatsphäre von Bürgern beinhaltete. Ein solcher schwerwiegender Eingriff würde zwingend eine Regelung in einem formellen Gesetz voraussetzen (mehr dazu unten bei den Ausführungen zu Art. 24b des Entwurfs).

Hinzu kommt, dass die Verordnung, wie im Folgenden zu zeigen sein wird, auf technischer Ebene mehr Fragen aufwirft, als sie beantwortet. Anstatt die Verordnung an den Informationsbedürfnissen der Strafverfolgung zu orientieren, wird zudem versucht, technische Lösungen in einem bestimmten technologischen Umfeld zu beschreiben und eine Reihe von Parametern, oft in unklarem Kontext, aufzulisten (dazu den Technischen Annex dieses Dokuments, S. 1).

Da nach Auffassung der asut vor einer Revision der VÜPF der Abschluss der Revision des BÜPF mit dem normalen Durchlauf des Gesetzgebungsverfahrens nötig wäre, wird auf einen detaillierten Änderungsvorschlag verzichtet. Wegen der unklaren, bzw. inexistenten formell-gesetzlichen Grundlage müsste dieser ohnehin nur Stückwerk bleiben. Die asut hat sich bei der BÜPF-Revision schon bisher sehr kooperativ gezeigt und hat mit konstruktiven Vorschlägen an dieser mitgewirkt. Sie wird dies selbstverständlich auch künftig tun und zu einer erfolgreichen Umsetzung jenes Projekts Hand bieten.

1.6 Fehlende Berücksichtigung des Verhältnismässigkeitsprinzips in der Verordnung

Es wäre zu berücksichtigen, dass bei Anbietern mit geringer Kundenzahl, bei Anbietern mit überwiegendem Anteil an Business-Kunden oder aber bei seltenen Überwachungsarten im Hinblick auf die in diesen Fällen nur kleine Zahl von zu erwartenden Überwachungsvorgängen eine Installation von Überwachungsanlagen unverhältnismässig und nicht zumutbar scheint. Die neuen Richtlinien TR TS müssten in diesem Sinne neben den Handover Interfaces (HI), entsprechende Schnittstellen (in ETSI Terminologie Internal Network Interface, INI) spezifizieren, dass der ÜPF in vergleichbaren Fällen ad hoc Ausrüstung installieren kann. In solchen Fällen dürfen die FDA allenfalls verpflichtet werden, die für die Installation der Ausrüstung nötigen Schnittstellen zur Verfügung zu stellen, nicht aber, die Anlagen als solche „auf Vorrat“ zu beschaffen.

Ebenfalls eine klare Verletzung des Verhältnismässigkeitsprinzips liegt in der Anforderung von Art. 18 Abs. 3 vor, eine 24x7-Erreichbarkeit sicherzustellen. Viele kleine Provider beschäftigen nur wenige Angestellte und wären durch eine derartige Anforderung überfordert.

1.7 Fehlende Entscheidgrundlage für eine Ausweitung der Überwachungspflichten

Abschliessend ist darauf hinzuweisen, dass die Ausweitung des Anwendungsbereichs der VÜPF offenbar erfolgt, ohne dass über die Wirksamkeit der bisherigen Überwachungsmassnahmen Statistiken erhoben worden wären. Schon die Wirksamkeit der bisherigen Methoden bleibt vielmehr völlig im Unklaren, und erst recht ist nicht gesichert, ob von der geforderten Ausweitung der Überwachungsarten überhaupt die erwünschte Wirkung zu erwarten sei. Umgekehrt betrachtet bleibt also völlig offen, ob für die mit der Vorlage neu eingeführten schweren Eingriffe in die Privatsphäre der Bürger eine sachliche Grundlage besteht.

Auch dies spricht deutlich für die Forderung der asut, die Verordnungsrevision aufzuschieben, bis einerseits die Revision des zu Grunde liegenden Gesetzes erfolgt ist, und andererseits gestützt auf zuverlässiges Datenmaterial über weitere Überwachungsmassnahmen zu entscheiden wäre.

Leider ist es in der Vorlage nicht gelungen, eine genügende Rechtssicherheit hinsichtlich dem *persönlichen und sachlichen Anwendungsbereich* wie den Rechtsunterworfenen und den Überwachungsmassnahmen bzw. –typen zu erreichen, da gewisse Bestimmungen zu offen formuliert worden sind bzw. die Definitionen nicht hinreichend klar sind.

So hatte bereits VE BÜPF in Art. 1 hinsichtlich des *sachlichen Anwendungsbereiches* den Mangel, dass der Begriff des *Internetverkehrs* - als Teilmenge des Fernmeldeverkehrs - *namentlich* Mail und Internettelefonie – nicht hinreichend klar definiert war und z.B. offen lies, ob weitere auf TCP/IP basierender Dienste wie HTTP, FTP, Telnet etc. resp. Software, welche auf diesen Diensten aufbaut (z.B. Webbrowser, Newsreader, FTP-Client etc.) zum Internetverkehr im Sinne des Gesetzes zählen werden oder nicht.

Genauso unklar ist der Begriff des *Internets* bzw. der Begriff der *Anwendungen* im vorliegenden Entwurf zum VÜPF. Art. 24 Abs. 2 lit a und b E VÜPF nehmen Postdienste und Multimediadienste in einer nicht abgeschlossenen Aufzählung auf. Damit wird auf Verordnungsstufe der sachliche Anwendungsbereich erweitert, was aber einer gesetzlichen Grundlage bedürfte und somit im BÜPF zu regeln wäre. Zudem ist im Rahmen der Rechtssicherheit eine abschliessende Liste zu definieren; *eine Aufzählung mit usw. ist nicht hinreichend für die Legitimation des Eingriffes in Grundrechte.*

Betreffend dem persönlichen Anwendungsbereichs hinsichtlich Internet ist die Begriffsdefinition „*Internet-Anbieterin*“ bei den Begriffen und Abkürzungen relevant. *Aufgrund der derzeitigen Formulierung wären Dienste innerhalb einer Closed-User-Gruppe deshalb nicht erfasst, was vor dem Gesagten auch richtig erscheint.*

2 Zu einer Auswahl an einzelnen Bestimmungen

2.1 2. Abschnitt: Bearbeitung von Personendaten (…)

Zu Art. 9 Abs. 2: “Übergabepunkt”

Die Frage der Bestimmung der Übergabepunkte ist nach wie vor ungelöst. Damit ist offen, für welchen Abschnitt die Provider genau verantwortlich gemacht werden sollen. Ausserdem ist unklar, welche Aspekte unter Datensicherheit fallen sollen (Confidentiality, Authentication, Availability (DoS), Integrity, Non-repudiation). Zu beiden Punkten vgl. auch den Technischen Annex, S. 4 f.

2.2 4. Abschnitt: Überwachung der „Telefondienste“

Die Abgrenzung des Fernmeldeverkehrs vom Internetverkehr bleibt unklar. Internet-Technologie (damit ist eine Protokollarchitektur gemeint) kann ausserhalb des Internet eingesetzt werden beispielsweise in einem Carrier Class IP Netz (z.B. für VoIP). Vgl. dazu die Anmerkung im Technischen Annex, S. 8.

Zu Art. 16:

In der bisherigen Verordnung wurde unterschieden zwischen „Überwachung des Fernmeldeverkehr mit Ausnahme von Internet“ und „Überwachung der Internetzugänge“. Neu heisst es nun im 4. Abschnitt nur noch „Überwachung der *Telefondienste*“ und später im 6. Abschnitt „Überwachung des Internets“.

Die genaue Terminologie müsste nochmals überprüft werden, wird doch im weiteren Verlauf des 4. Abschnitts nicht mehr von „Telefondiensten“, sondern wieder von „Fernmeldeverkehr“ gesprochen.

Sodann sollten keine Erhebungen gemacht werden über netzinterne Parameter wie IMSI, reale Cell IDs, usw. Solche Erhebungen sind für die Strafverfolgungsbehörden und die Gerichte nicht beweisrelevant. Die Parameter werden nur netzintern verwendet und dienen der Kundensicherheit sowie zur Sicherstellung der Netzintegrität. Bei einigen solcher Daten, wie z.B. den realen Cell IDs, handelt es sich zudem um geschäftsrelevante Daten, welche die FDA nicht herausgeben können, ohne Geschäftsgeheimnisse zu verletzen.

Im Weiteren ist darauf hinzuweisen, dass viele der für die Erhebung vorgesehenen Parameter genau besehen kaum jene Beweissicherheit bieten, die sich der Verordnungsgeber offenbar vorstellt. Vielfach sind die Parameter nämlich durch die Endkunden einfach änderbar (z.B. die MAC-Adresse), sodass sie, weil sehr schwierig verifizierbar, gar keine zuverlässige Beweisführung erlauben. Entsprechend ist deren Erhebung für die Strafverfolgungsbehörden und Gerichte nicht von Nutzen und damit auch unverhältnismässig. Die Erhebung sehr schwierig verifizierbarer Parameter führt im besten Fall zu Beweislosigkeit, im schlechteren Fall zu nicht gerechtfertigten Anschuldigungen oder gar Festnahmen. Entsprechend ist zu fordern, dass Richtlinien zur Verifizierbarkeit von Parametern bestehen und die diesbezügliche Verantwortung einzelner FDA klar umschrieben wird, basierend auf ETSI TR 187 012 clause 5.2 und Draft ETSI TS 187 017 clause 4.

SIM-Nummern sind sodann keine auf dem Netz verfügbaren Parameter, welche zu den Fernmeldeverkehrsdaten gehören. Die Information der SIM-Nummern gehört zu den Auskünften über Fernmeldeanschlüsse und wird heute schon durch eine Anfrage über das CCIS angefragt und die Auskunft durch die FDA erteilt.

In Art. 16 Bst. d Ziff. 2 ist im Weiteren keine klare Zuteilung der Parameter in Klassen gegeben. Zudem erzeugt die Formulierung „(wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer)“ Rechtsunsicherheit, da nicht festgelegt ist, welche weiteren Angaben unter dieser Bestimmung herausverlangt werden könnten.

Zu Art. 16 lit. e: Antennensuchlauf:

Diese Ergänzung darf an dieser Stelle keinesfalls gemacht werden, wenn schon müsste die Durchführbarkeit von Antennensuchläufen im Gesetz im formellen Sinn vorgesehen werden, da diese Massnahme klar gegen die geltende Strafprozessordnung verstösst, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen, sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmte Anschlüsse (dazu schon vorne 1.3).

Darüber hinaus lässt sich sagen, dass es gar nicht möglich ist „an einem bestimmten Standort“ rückwirkend „alle mobilen Kommunikationsvorgänge“ zu eruieren. Es liesse sich höchstens eine grössere oder kleinere Zahl an Funkzellen ermitteln, welche „einen bestimmten Standort“ mit einer gewissen Wahrscheinlichkeit versorgen, und anschliessend die Kommunikationen über diese Funkzellen in einem definierten Zeitraum ermitteln. Ob sich aber die gesuchte Kommunikation darunter befindet, ist nicht gewährleistet.

Zu Art. 16 und 16a vgl. zudem die Anmerkungen im Technischen Annex, S. 9f.

Zu Art. 16b Überwachungsmassnahmen mit Auslandsbezug

Mit der Einfügung dieser Norm sollen die sog. internationalen „Kopfschaltungen“ verankert werden, das heisst, die FDA sollen dazu verpflichtet werden, ausländische Rufnummern, respektive schweizerische Rufnummern im Ausland (outbound Roamer) überwachen zu können, wenn diese mit ihren Kunden kommunizieren. Diese Bestimmung ist abzulehnen, obschon das Bundesverwaltungsgericht vor rund zwei Jahren entschieden hat, eine solche Massnahme sei rechtmässig. Das Bundesverwaltungsgericht (A-2335/2008) stellte sich auf den Standpunkt, dies sei im Prinzip das Gleiche wie die Überwachung einer

inländischen Nummer, jedenfalls sei ja die überwachte Nummer klar bestimmt. Allerdings übersah das Bundesverwaltungsgericht die Tatsache, dass es sich

- entweder um eine Überwachung einer Person im Ausland handelt, welche nach Abschluss des Verfahrens nicht, wie von der Gesetzgebung vorgesehen, über die Vornahme der Überwachung informiert werden kann, und die darüber hinaus gegen das Territorialitätsprinzip verstösst,
- im Prinzip auch um eine Überwachung von unbestimmt vielen Personen im Inland handelt, welche Kommunikationen mit der genannten Nummer im Ausland haben. Auch die Kopfschaltung widerspricht damit dem Grundkonzept des BÜPF, wonach Fernmeldeüberwachungen nicht zur Suche nach Verdachtsmomenten gegen unbestimmt viele Personen durchgeführt werden dürfen (Rasterfahndung), sondern nur im Falle eines bereits vorliegenden Verdachts und nur betreffend bereits im Voraus klar bestimmte Anschlüsse. Auch hier ist zudem offensichtlich, dass die unbestimmte Anzahl an Personen im Inland nach Abschluss des Verfahrens nicht über die Überwachung informiert werden kann.

Entgegen der Ansicht des Bundesverwaltungsgerichts gibt es also doch starke Anzeichen dafür, dass Kopfschaltungen nicht ins Konzept des aktuellen BÜPF passen, weshalb auch die Entscheidung über die Zulässigkeit von Kopfschaltungen dem Gesetz im formellen Sinn anheimgestellt werden sollte und nicht im Rahmen einer Revision der VÜPF erfolgen darf.

Zu Art. 16b vgl. zudem die Anmerkungen im Technischen Annex, S. 11 f.

Zu Art. 17 Abs. 4

Es ist unklar was alles mit „Zuleitung“ gemeint ist. ETSI spezifiziert die Auslieferungsformate an einem Übergabeinterface (Handover Interface, HI), spezifiziert jedoch die Ausleitungsnetze (Delivery Networks) aus der Infrastruktur des Providers (IIF/MD) zur Infrastruktur von ÜPF (LEMF) nur oberflächlich. Wenn „die Spezifikationen dieser Zuleitung“ bedeuten würde, dass ÜPF Delivery Networks spezifiziert, würde dies einen erheblichen Eingriff in die Netzhoheit der Provider bedeuten.

Zu Art. 17 Abs. 5 und Art. 25 Abs. 5

Obschon der Verordnungsgeber (wie auch das Bundesverwaltungsgericht) davon ausgehen will, dass der Überwachungstypenkatalog der VÜPF abschliessend sei, soll diese Bestimmung nun vorsehen, dass auch nicht explizit in der Verordnung aufgeführte Fälle von Überwachungen möglich seien. Damit wird der Katalog der Überwachungstypen offengehalten, und es besteht keine Rechtssicherheit, was vom ÜPF an Überwachungen zu erwarten ist. Dies betrifft die Betreiber im Rahmen der in diesem Zusammenhang zu erwartenden Investitionen und den Normalbürger insofern, als er nicht weiss, wie er vom Staat überwacht werden kann. Gemäss Legalitätsprinzip müsste wenigstens ein Rahmen an zulässigen Überwachungen im Gesetz im formellen Sinn definiert werden. Was darüber hinaus geht, sollen die FDA nicht nur nicht ausführen müssen, sondern im Hinblick auf den Schutz der Freiheitsrechte der Bürger auch nicht ausführen *dürfen*. Daher ist diese Spezialfallregelung abzulehnen, jedenfalls solange, als nicht mit einer zufriedenstellenden BÜPF-Revision eine Grundlage geschaffen wird, welche den Rahmen der Behördenpraxis klar vorgibt.

Zu Art. 17 vgl. zudem die Anmerkungen im Technischen Annex, S. 12 f.

Zu Art. 18

Auf die Unverhältnismässigkeit der Anforderung von Art. 18 Abs. 3 (permanente Erreichbarkeit) wurde bereits unter Ziff. 1.6 hingewiesen.

Die Änderungen, v.a. in den Absätzen 7 und 8, betreffen Spezialwünsche des ÜPF. Eine Gratisnutzung der Fernmeldedienste der FDA durch den ÜPF ist abzulehnen, zumal eine solche Nutzung in keiner Weise eingegrenzt wäre. .

Auch die begehrten Unterstützungsleistungen hinsichtlich der Frage, ob tatsächlich die richtige Person überwacht werde, sind fragwürdig, da diese Begehren des ÜPF daher rühren, dass er in letzter Zeit bewährte Überwachungsmethoden durch billigere und unzuverlässige Methoden ersetzt hat. Abs. 8 lässt

zudem völlig offen, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um die entsprechende Unterstützung leisten zu können.

Vgl. auch zu Art. 18 die weiter gehenden Anmerkungen im Technischen Annex, S. 13 f.

Zu Art. 19a der *bestehenden* Verordnung

Art. 19a der bestehenden VÜPF bleibt nach dem Entwurf unverändert. Die Norm bestimmt, dass die FDA sicherstellen müssen, dass beim Verkauf von Prepaid-SIM-Karten die Personalien der Kundinnen und Kunden anhand eines *für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes* erfasst werden. Nach Auffassung der asut wäre hier jedoch eine Änderung vorzunehmen.

Nimmt man die geltende Bestimmung beim Wort, können Asylbewerber mit Asylbewerberausweis (Ausländerausweis F, N und S) keine Prepaid-Karten beziehen, weil dieser Ausweis nicht zum Grenzübertritt berechtigt (vgl. Hansjakob, Kommentar, N 3 zu Art. 19a VÜPF). Nach Auffassung der asut ist das Kriterium der Eignung zum Grenzübertritt jedoch unsachlich, ist doch nur die Eignung zur Identifikation, nicht aber die Möglichkeit zum Grenzübertritt für den Zweck von Art. 19a VÜPF relevant.

Das Migrationsamt schiebt für das Verbot der Verwendung von F-, N- und S-Ausweisen sodann die Begründung nach (http://www.uvek.admin.ch/themen/kommunikation/00950/00951/index.html?lang=de, Frage 16), dass die entsprechenden Ausweise oftmals auf falsche Namen ausgestellt würden, weil sie nur auf den Angaben der Asylbewerber basieren und nicht auf amtlichen Dokumenten von deren Heimatland. Aus Sicht der asut ist es jedoch unverhältnismässig, die Verwendung von Ausweisen F, N und S bloss aufgrund eines möglichen Fehlverhaltens einzelner Ausweisträger zu beschränken. Abgesehen davon wäre die Identifikationseignung eines F-, N- oder S-Ausweises selbst dann nicht in Frage gestellt, wenn der Ausweis auf falschen Angaben des Asylbewerbers basierte, ist doch der Asylbewerber auch unter dem entsprechenden (falschen) Namen registerlich erfasst, sodass er gerade auch anhand des falschen Namens zweifelsfrei ausfindig gemacht werden könnte.

Diese Situation ist immer noch besser als jene, dass Asylbewerber für die Nutzung von Mobiltelefonie gezwungen wären, einen Strohmann vorzuschicken, denn in diesem Fall wäre die Identifikation gar nicht mehr gewährleistet.

Träger der Ausweise F, N und S haben zudem in der Regel nicht die Möglichkeit, die für Postpaid-Angebote von Ausländern aus Sicherheitsgründen geforderten Depotzahlungen zu leisten. Ein Verbot, Prepaid-Karten zu beziehen, läuft damit auf eine unverhältnismässige Verletzung Kommunikationsfreiheit der entsprechenden Individuen hinaus. Entsprechend wäre bei einer Verordnungsrevision der in Art. 19a verwendete Ausweisbegriff um Ausweise F, N und S zu erweitern.

2.3 6. Abschnitt: Überwachung des Internets

Zunächst bleibt unklar, wofür der Ausdruck „Internet“ verwendet (dazu die Anmerkungen im Technischen Annex, S. 16 f.) wird.

Zu Art. 23

Der Inhalt der Norm ist bezüglich Inhalt und Beschreibungstiefe mit Art.15 Abs. 1 abzugleichen (vgl. den Technischen Annex, S. 17).

Erneut ist darauf hinzuweisen, dass eine Datenherausgabe betreffend sämtlicher Netzparameter (Bst. g), welche nicht überwachungsrelevant sind und welche reine Netzdaten der betreffenden FDA bilden, nicht akzeptabel ist (dazu vorne 2.2)

Zu Art. 24

Art. 24 sieht eine massive Ausdehnung des Katalogs der Überwachungsarten vor. Die asut ist der Auffassung, dass eine derartige Ausdehnung keine genügende Rechtsgrundlage in Art. 15 BÜPF findet, zumal die meisten der entsprechenden Überwachungsarten zum Zeitpunkt der Verabschiedung von Art. 15 BÜPF noch nicht im Fokus des Gesetzgebers waren. Dementsprechend ist die geplante Ausweitung des Katalogs der Überwachungsarten durch die Delegationsnorm in Art. 15 Abs. 6 BÜPF nicht gedeckt. Die asut

ist der Auffassung, eine Erweiterung des Katalogs der Überwachungsarten sei ausschliesslich auf Grund eines Gesetzes im formellen Sinn zulässig.

Eine Überwachung von VPN (Art. 24 Bst. f) wäre in jedem Fall explizit auf Anbieter zu beschränken, die VPN selber anbieten, und nicht auf die Access Provider, die VPN-Datenströme bloss von ihren Endkunden zu VPN-Anbietern im Internet weiterleiten. Dies bereits daher, weil VPN-Daten verschlüsselt und damit für eine Ausleitung ungeeignet sind.

Art. 24 Abs. 2 sieht zudem neu auch Überwachungen auf der Anwendungsebene des Internets vor (für VoIP, Instant Messaging, Multimediadienste, etc.). Die bisherige Praxis wie auch die Literatur gehen klar davon aus, dass das BÜPF auf Access Provider anwendbar ist, nicht aber auf Service Provider (Anwendungsanbieter; vgl. Hansjakob, Kommentar, N 24 zu Art. 1 BÜPF). Auch diese Norm sprengt den durch Art. 15 BÜPF vorgesehenen Rahmen daher klar, selbst die Definition der Internetanbieter nach Ziff. 1 des Anhangs der Verordnung umfasst derartige Anwendungsanbieter nicht.

Die Belastung von Anwendungsanbietern führte im internationalen Vergleich zu einer erheblichen Wettbewerbsverzerrung und vor allem zu einer Beeinträchtigung der Innovation im Bereich der Internetanwendungen, weil die Entwickler mit (im Vergleich zu den allgemein niedrigen Entwicklungskosten für die Anwendungen) ganz erhebliche Mehrkosten für die Entwicklung von Überwachungsschnittstellen einplanen müssten. Die Innovation von Anwendungen des Internets, gerade auch im Mobilfunk (Smartphones), geht heute sehr rasch voran, und entsprechend profitiert die Gesellschaft vom Internet als einem wahren Motor des Fortschritts. Diese Dynamik soll nicht durch eine übertriebene Überwachungspflicht gehemmt werden..

Im Weiteren lässt der Entwurf – und hier liegt ein weiterer schwerwiegender Kritikpunkt – völlig offen, wer für die Überwachung von Anwendungen wie VoIP, Instant Messaging oder Multimediadienste verantwortlich wäre. Angesichts dessen, dass die Access Provider bisher keinerlei technische Möglichkeiten zur Filterung von Inhalten (Deep Packet Inspection) haben, und angesichts dessen, dass eine solche Filterung in der Regel Know-How über Kommunikationsprotokolle höherer Schichten als jener des Access und allfällige Verschlüsselungsmechanismen voraussetzt, das nur der Anbieter der Anwendung selber besitzt, scheint die Vorstellung, dass die Access Provider für eine Ausleitung von aus dem Datenstrom eines Kunden ausgefilterter Anwendungsdaten verantwortlich sein sollen, nicht haltbar. Wollte man Anwendungen doch in die VÜPF aufnehmen, so müsste daher zumindest klargestellt werden, dass für die Ausleitung entweder die Anwendungsanbieter oder dann der ÜPF, nicht aber die Access Provider verantwortlich sein können. Der ÜPF muss auch dann die Filterung übernehmen, wenn die Anwendungsanbieter vom Ausland aus tätig sind und dementsprechend nicht selber dem BÜPF unterstehen (dazu Hansjakob, Kommentar, N 26 zu Art. 1 BÜPF). Technisch gesprochen darf die Überwachungspflicht der Access Provider daher nur die IP-Adresselemente, aber nicht in der IP-Payload gespeicherte Adresselemente enthalten.

Vgl. zu Art. 24 auch den Technischen Annex, S. 18 f.

Zu Art. 24a Überwachungstypen (Echtzeit)

Die Artikel 24a und 24b enthalten einen umfassenden, schwerwiegenden Ausbau an Datenlieferungspflichten, welcher für die FDA einschneidende Folgen hätte. Gemäss BÜPF/StPO ist an sich nur vorgesehen, dass die FDA den gesamten Fernmeldeverkehr von bestimmten Anschlüssen zuleiten müssen.

Die Bestimmung enthält (wie Art. 24b auch) einige Anforderungen, wonach für die Überwachung und Beweisführung im Strafverfahren überhaupt nicht relevante Daten herauszugeben wären, was teils sogar die Netzintegrität der FDA tangieren würde (wie IMSI, reale Cell ID, usw.)

Unklar bleibt ferner der Inhalt von Art. 24a Bst. b Ziff. 3, der von „Anmeldungsdaten“ spricht. Die Norm wäre dahin zu präzisieren, dass, falls überhaupt, ausschliesslich Login-Daten für die Anmeldung im Netz des Access Providers, nicht aber Login-Daten für die Anwendungsebene des Internet (http, etwa für E-Banking, E-Mail-Accounts etc.) unverschlüsselt ausgeleitet werden. Login-Daten (Username plus Password) sind Credentials (Berechtigungsnachweise) und von ihrer Eigenschaft her nicht geeignet, eine Straftat zu begehen. Jede Dritte Entität, die über die Credentials einer Entität verfügt, kann in ihrem Namen, d.h. mit ihren Identitäten kommunizieren. Damit gehören Login-Daten in dieselbe Kategorie wie die IMSI. Die Ausleitung von Login-Daten der Anwendungsebene hätte erstens zur Bedingung, dass die Provider zu einer

detaillierten Filterung des Internetverkehrs (Deep Packet Inspection) gezwungen würden, was hohen Investitionsbedarf mit sich brächte, und würde zweitens den Zweck der Fernmeldeüberwachung, nämlich die Inhalte von Kommunikation zu Tage zu fördern, überdehnen. Denn damit würde es den Strafverfolgern auch möglich, leicht etwa Banktransaktionen von Verdächtigen nachzuvollziehen. Abgesehen davon, sind Login-Daten einer Client zu Server Beziehung auf Anwendungsebene verschlüsselt und können durch den Access Provider nicht offengelegt werden. Für solche Aufgaben ist die Fernmeldeüberwachung aber nicht gedacht, geschweige denn fände sie im gegenwärtig geltenden BÜPF eine genügende gesetzliche Grundlage.

Unklar bleibt im Weiteren die Bestimmung in Art. 24a Bst. b Ziff. 4 hinsichtlich des Begriffs der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene beschränkt, oder will die Bestimmung etwa auch eine Ausleitung für die Anwendungsebene (http) einführen? Einmal mehr kann nach Auffassung der asut nur die IP-Ebene gemeint sein, nicht aber Adresselemente, die in der IP-Payload enthalten sind.

Art. 24b Überwachungstypen (rückwirkend)

In Art. 24b (betreffend rückwirkende Überwachung) wird ebenfalls ein systematischer Ausbau vorgenommen, sodass diese Datenlieferungspflicht mit der früheren Lieferung von schlichten Verkehrs- und Rechnungsdaten nichts mehr gemein hat.

Es wird auf die bereits bei Art. 24a geäusserte Kritik zur Echtzeitüberwachung von Anmeldungsdaten verwiesen. Sie gilt für die rückwirkende Speicherung der Daten erst recht, weil ausserhalb des Zugriffsbereichs des Endkunden gespeicherte Anmeldedaten ein lohnenswertes Ziel für Hackerangriffe bilden (die Erfahrung gerade der letzten Wochen und Monate zeigt, dass auch Behörden niemals für absolute Sicherheit der von ihnen gespeicherten Daten sorgen können). Eine Pflicht zur Speicherung solcher Daten würde damit Anwendungen wie E-Banking deutlich unsicherer machen, wenn nicht gar das Vertrauen des Publikums in sie zerstören.

Unklar bleibt im Weiteren analog zum bereits zu Art. 24a Gesagten in Art. 24b Bst. a Ziff. 4 der Begriff der Adressierungselemente: Ist die Bestimmung auf Adressierungselemente der IP-Ebene auf Seiten des Endkunden beschränkt, oder will die Bestimmung auch eine rückwirkende Herausgabe für die Anwendungsebene und der vom Endkunden besuchten IP-Adressen oder URLs einführen? Letzteres liefe auf eine Vorratsdatenspeicherung für das Internet hinaus (rückwirkende Herausgabe sämtlicher besuchter Websites etc.), die den Delegationsrahmen von Art. 15 BÜPF klar sprengen würde und als höchst problematischer politischer Entscheid klar in die Hände des Gesetzgebers gehört, und die – nebenbei gesagt – aus der aktuellen Vorlage für eine Revision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit BWIS eben erst wieder entfernt wurde. Eine Einführung einer Vorratsdatenspeicherung auf dem Verordnungsweg steht damit nach Auffassung der asut völlig ausser Frage.

Ferner ist der Begriff der periodischen Übermittlung unklar und näher zu umschreiben. Vgl. zu Art. 24 zudem auch den Technischen Annex, S. 19 ff.

Zu Art. 24c

Auch Art. 24c geht klar weiter als eine einfache Nachführung. Die Bestimmung will die FDA zu einer Art „Kopfschaltung“ im Internetbereich zwingen. Die Argumente zur Kopfschaltung wurden bereits dargelegt. Auch im Internetbereich kann es nicht angehen, ohne die vom BÜPF geforderte konkrete Verdachtsgrundlage mit einer Kopfschaltung „Fallen“ zu stellen, in die die Nutzer dann hereintappen. Vgl. dazu auch den Technischen Annex, S. 22 f.

Zu Art. 25-27

Vgl. zu diesen Artikeln ebenfalls die Anmerkungen im Technischen Annex (S. 23 ff.).

2.4 Definitionen

Die Definition der Internet-Anbieterin in Ziff. 1 des Anhangs der Verordnung, die allein auf die Verwendung von IP-Adressen abstellt (besser wäre ohnehin: das Internet Protocol IP), ist zu weit. Es gibt eine Reihe von Produkten, die mit IP arbeiten, aber keinen Zugang zum Internet vermitteln, denn IP ist eine universelle in Computernetzen verwendete Technologie, deren Einsatz – entgegen ihrer Bezeichnung – nicht auf das Internet beschränkt ist.

Dementsprechend wäre die Definition durch die Einführung eines Elements des Zugangs zum Internet enger zu fassen. Vgl. dazu auch den Technischen Annex, S. 2.

Gemäss Ziff. 8 des Anhangs besteht folgende Definition: Adressierungselemente: Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern (Art. 3 Bst. f des Fernmeldegesetzes vom 30. April 1997 9 - FMG). Die Target Identity ist beschränkt auf ein Nummerierungselement. „Adressierungselement“ in Art. 16b Abs. 2 ist damit zu ersetzen durch „Nummerierungselement“.

Gemäss Ziff. 9 des Anhangs wird der Begriff der Kommunikationsparameter definiert als die Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind (Art. 3 Bst. g FMG). Gemäss dieser Definition sind SIM-Nummer, IMSI, MSISDN Parameter, die mit dem Kunden assoziiert sind und der Identifikation der Person dienen und damit auch „Parameter zur Teilnehmeridentifikation“. Die IMEI ist mit einem Mobiledevice assoziiert und ist ein „Kommunikationsparameter des Endgerätes der Mobiltelefonie“. Der Begriff der SIM-Nummer ist zudem auch in ETSI TS 102 657 nicht definiert und damit unklar; in jedem Fall erlauben die durch ETSI definierten Datenformate nicht, eine SIM-Nummer auszuliefern.

Zu Ziff. 14 vgl. sodann den Technischen Annex, S. 32.

2.5 Kosten

Die gleichzeitig mit der VÜPF in Revision befindliche Verordnung über Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs sieht für eine Reihe von Überwachungsarten einen Wechsel von stundenbasierter Aufwandsentschädigung hin zu Entschädigungspauschalen vor. Dies droht zu einer signifikanten Reduktion der Entschädigungen zu führen. Angesichts dessen, dass den FDA nach offiziellen Studien nur gut 30% der Überwachungskosten entschädigt werden, lehnt die asut eine weitere Reduktion strikte ab. Immerhin werden andere Unternehmen, die den Untersuchungsbehörden bei der Polizeiarbeit behilflich sind – etwa private Bewachungsunternehmen – auch nicht nur zu 30% entschädigt.

Wie bereits erwähnt, bilden die Entschädigungen zudem einen wesentlichen Streitpunkt auch in der gegenwärtigen Revision des BÜPF. Als eminent politische Materie sind sie zumindest in den Grundzügen auf dem Weg der Gesetzgebung festzulegen und nicht durch eine Verordnungsrevision.

Sodann wären auch auf Verordnungsebene klare Kriterien vorzusehen, in welchen Fällen eine pauschalisierte Entschädigung zulässig ist und wann eine Entschädigung nach Aufwand zu bezahlen ist. Keinesfalls kann eine derartige Entscheidung an den ÜPF delegiert werden, wie dies der neue Art. 4a der Gebührenverordnung offenbar will.

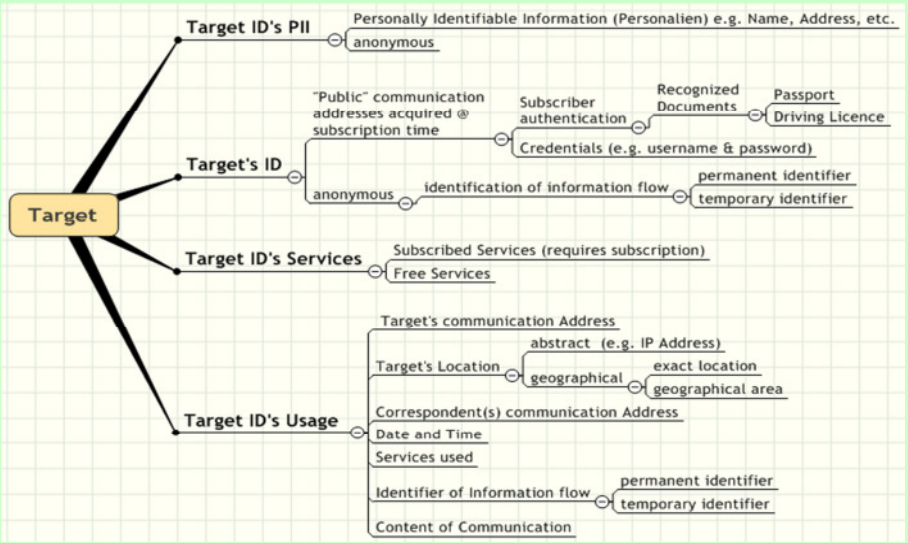
Auf die Auswirkungen der Erweiterung des Katalogs der Überwachungsarten auf die Entschädigungen für die FDA wurde bereits vorne unter 1.2 hingewiesen.

In Art. 4a der Gebührenverordnung ist ferner zunächst die Rede von CHF 160.- pro Stunde, dabei sollen die Entschädigungen gemäss Absatz 4 bloss 80% des Zeit- und Sachaufwandes decken. Dies ist widersprüchlich oder zumindest unklar.

Bern, 29. Juli 2011

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

Technik-asut: Zusammenfassend wird festgestellt, dass VÜPF keine klaren Strukturen hat um darzulegen, was Strafbehörden von Providern wissen wollen, wie dies beispielsweise in der unterstehenden Darstellung ausgedrückt wird (dazu kommen noch die Rechnungsdaten).



Anstatt in der Verordnung an Informationsbedürfnissen der Strafverfolgung zu orientieren, wird versucht, technische Lösungen in einem bestimmten technologischen Umfeld zu beschreiben und eine Reihe von Parametern, oft in unklarem Kontext, aufzulisten. Für die technische Umsetzung sind die Technischen Richtlinien einzusetzen, die durch starke Anlehnung an ETSI den verpflichteten Providern gestatten, Weltmarktprodukte ihrer Lieferanten einzusetzen und damit das Gesetz mit kostengünstigen Lösungen zu erfüllen.

Die VÜPF wurde im Jahr 2001 geschrieben vor den Hintergrund des traditionellen Telefondienstes, ergänzt mit E-mail; durch die punktuellen Anpassungen kann der rasanten Entwicklung der Technologie und der neuen Rollenteilung der verschiedenen Provider nicht Rechnung getragen werden.

vom 31. Oktober 2001 (Stand am 1. September 2007)
Änderung vom …2011

Der Schweizerische Bundesrat, gestützt auf Artikel 17 des Bundesgesetzes vom 6. Oktober 2000[1] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), *verordnet:*

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Geltungsbereich

1 Diese Verordnung regelt die Organisation und das Verfahren zur Überwachung des Post- oder Fernmeldeverkehrs sowie die Erteilung von Auskünften über die Fernmeldeanschlüsse.

2 Sie gilt für:

a. den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst);
b. die anordnenden Behörden;
c. die Genehmigungsbehörden;
d. die Anbieterinnen von Postdiensten;
e. die Anbieterinnen von Fernmeldediensten, einschliesslich die Internet- Anbieterinnen;
f. die Betreiberinnen von internen Fernmeldenetzen oder Hauszentralen.

Art. 2 Begriffe und Abkürzungen

Die in dieser Verordnung verwendeten Begriffe und Abkürzungen sind im Anhang definiert**.**

Art. 3 Dienst

1 Der Dienst ist dem Eidgenössischen Justiz- und Polizeidepartement (Departement) administrativ zugewiesen.[4]

2 Er ergreift die notwendigen Massnahmen, um, innerhalb und ausserhalb der Dienstzeit, die Überwachungsanordnungen empfangen und die Prüfung nach Artikel 11 Absatz 1 Buchstabe a und Artikel 13 Absatz 1 Buchstabe a BÜPF durchführen zu können.

Art. 4 Meldung der Namen der zuständigen Behörden

Die Kantone und die zuständigen Bundesämter melden dem Dienst den Namen:

a. der Behörden, die zur Anordnung einer Überwachung zuständig sind;
b. der Genehmigungsbehörde;
c. der Behörden nach Artikel 14 Absatz 2 Buchstaben b und c BÜPF, die Auskünfte über Fernmeldeanschlüsse verlangen können.

Art. 5 Einreichung der Überwachungsanordnung beim Dienst

1 Die anordnende Behörde kann die Überwachungsanordnung beim Dienst einreichen:

a. per Post, per Telefax oder mit einem anderen durch das Departement zugelassenen sicheren Übertragungsmittel;
b. mündlich, in dringlichen Fällen.

2 Wenn sie die Überwachung mündlich anordnet, erhält sie die Nutzinformationen, die Verkehrs- und Rechnungsdaten sowie weitere Auskünfte über den Post- oder Fernmeldeverkehr einer Person erst, nachdem sie die Überwachungsanordnung mit einem Übertragungsmittel nach Absatz 1 Buchstabe a bestätigt hat.

3 Die anordnende Behörde reicht ebenfalls jede Abänderung oder jede Verlängerung der Überwachungsanordnung sowie jede gemachte Ergänzung mit einem Übertragungsmittel nach Absatz 1 Buchstabe a beim Dienst ein.

Art. 6 Mitteilung des Entscheids der Genehmigungsbehörde

Die Genehmigungsbehörde teilt dem Dienst ihren Entscheid mit den allfälligen zusätzlichen Vorkehren zum Schutz der Persönlichkeit umgehend, schriftlich mit.

2. Abschnitt: Bearbeitung von Personendaten im Rahmen der Überwachung des Post- oder Fernmeldeverkehrs

Art. 7 Kontrolle der Ausführung der Überwachungsanordnungen

1 Die Behörden, die Überwachungen anordnen oder genehmigen, sowie die Anbiete- rinnen von Post- oder Fernmeldediensten können diejenigen Personendaten bearbeiten, die sie für die Kontrolle der Ausführung der Überwachungsanordnungen benötigen.

2 Der Dienst führt eine Geschäftskontrolle über:

a. die Durchführung der Überwachungen von Post- oder

Fernmeldediensten;
b. die Gebühren und Entschädigungen.

Art. 8 Verarbeitungszentrum

1 Der Dienst errichtet und betreibt ein Verarbeitungszentrum für die Daten aus der Überwachung des Fernmeldeverkehrs- und der Kommunikation im Internet.

Technik-asut: Es ist unklar, wofür der Ausdruck Internet verwendet wird, d.h. für:

a) "The Internet" wobei man behaupten könnte, dass jeder der als "Vernetzer" und/oder "Hoster" auftritt, Mitglied der "Internet Community" ist;
b) Ein Netz in IP-Technologie, dessen Kommunikation nie in "The Internet" verlaufen muss, aber bei Nomadisierung in "ferne Länder" kann.

SIEHE KOMMENTAR ZU ABSCHNITT 6

2 Das Verarbeitungszentrum muss rund um die Uhr einsatzfähig sein, um:
a. die durch die Anbieterinnen von Fernmeldediensten gelieferten Daten aus der Überwachung des Fernmeldeverkehrs entgegenzunehmen und in einem Informationssystem aufzuzeichnen;
b. die Daten für die betroffene Strafverfolgungsbehörde bereitzustellen.

3 Der Dienst macht die Daten der Überwachung der Behörde zugänglich, die als
Empfängerin der Überwachungsdaten vorgesehen ist.

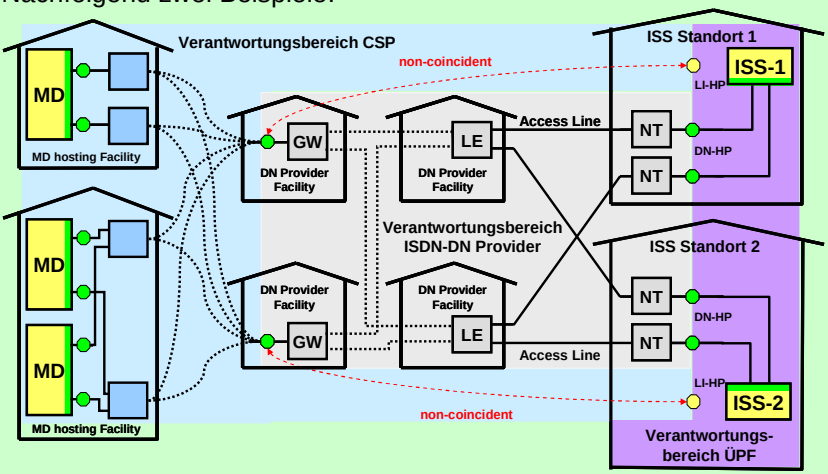
4 Der Dienst kann dieser Behörde die Daten auch in einer anderen Form übermitteln.

Art. 9 Datensicherheit

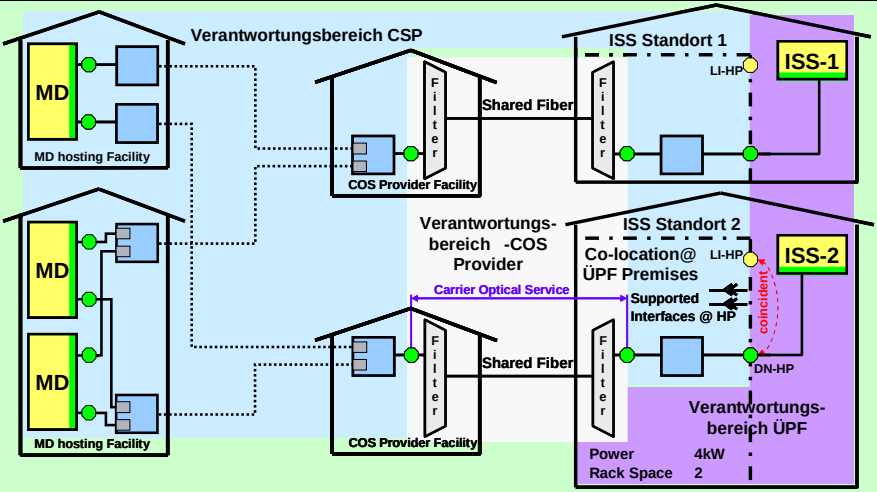
1 Für die Gewährleistung der Datensicherheit gelten die Verordnung vom 14. Juni 1993[5] zum Bundesgesetz über den Datenschutz und die Artikel 14 und 15 der Verordnung vom 23. Februar 2000[6] über die Informatik und Telekommunikation in der Bundesverwaltung.

2 Die Anbieterinnen von Post- oder Fernmeldediensten folgen den Anweisungen des Dienstes für die Datensicherheit bezüglich der Übertragung der Überwachungsdaten. Sie sind für die Datensicherheit bis zum Übergabepunkt der Daten an den Dienst verantwortlich.

Technik-asut: Die Frage der Bestimmung der Übergabepunkte ist nach wie vor ungelöst. Damit ist offen, für welchen Abschnitt Provider verantwortlich gemacht werden sollen. Ausserdem ist unklar, welche Aspekte unter Datensicherheit fallen sollen (Confidentialty, Authentication, Availability (DoS), Integrity, Non-repudiation).
In der Publikation „Ausleitungskonzept zwischen CSP und ISS“ spricht ÜPF von einem physikalischen und logischen Übergabepunkt, ohne eine Definition zu liefern. Anlässlich der Diskussionen des Ausleitungskonzeptes (dieses soll gemäss der Aussage von ÜPF an der Sitzung des erweiterten Kernteams ISS vom 30. Juni 2011Ende Juli 2011 erscheinen) wurde offensichtlich, dass eine Definition schwierig ist, weil es mehrere Übergabepunkte gibt und diese auf der Netzwerkebene (grün in Beispielfiguren) und der „Datenformat“-Ebene (gelb in Beispielfiguren). Nachfolgend zwei Beispiele:



Übergabepunkte und Verantwortungsbereiche im ISDN Delivery Network



Übergabepunkte, Verantwortungsbereiche und Leistungen bei der I -COS Lösung

Art. 10 Vernichtung der Daten

1 Der Dienst vernichtet die Überwachungsdaten, nachdem er sie den Behörden nach Artikel 8 Absätze 3 oder 4 übergeben hat, spätestens aber drei Monate nach der Einstellung der Überwachung.

2 Er vernichtet die Daten aus der Geschäftskontrolle ein Jahr nach Einstellung der
Überwachung.

3 Der Artikel 962 des Obligationenrechts[7] und die Gesetzgebung über die Archivierung bleiben vorbehalten.

3. Abschnitt: Überwachung des Postverkehrs

Art. 11 Überwachungsanordnung

Die beim Dienst eingereichte Überwachungsanordnung muss die folgenden Angaben enthalten:

a. den Namen der anordnenden Behörde;
b. den Namen der Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist;
c. soweit diese Daten bekannt sind: die Namen, Adressen und Berufe der tatverdächtigen Personen und der allenfalls zu

überwachenden weiteren Personen;
d. im Fall von Personen, die einem Berufsgeheimnis nach Artikel 271 Absatz 1 der Strafprozessordnung2 (StPO) unterstehen: einen Vermerk über diese Besonderheit;
e. die Straftat, die mit der Überwachung aufgeklärt werden soll;
f. den Namen der Postdienst-Anbieterin und, wenn möglich, den Namen der mitwirkenden Poststellen;
g. die angeordneten Überwachungstypen;
h. wenn nötig, die weiteren Auskünfte über den Postverkehr einer Person und die Anträge auf zusätzliche Vorkehren zum Schutz der Persönlichkeit;
i. den Beginn und die Dauer der Überwachung.

Art. 12 Überwachungstypen

Folgende Überwachungstypen können angeordnet werden:
a. das Abfangen der Postsendungen (Echtzeit-Überwachung);
b. die Lieferung folgender Daten über den Postverkehr (Echtzeit-Überwachung), soweit diese Daten verfügbar sind:
   1. die Identität der Empfängerinnen und Empfänger der Postsendungen,
   2. die Identität der Absenderinnen und Absender der Postsendungen,
   3. die Art der Postsendungen,
   4. den Zustellungsstand der Postsendungen;
c. die Lieferung folgender Verkehrs- und Rechnungsdaten (rückwirkende Überwachung):
   1. für Postsendungen mit Zustellnachweis: die Empfängerin oder den Empfänger, die Absenderin oder den Absender und die Art der Postsendung sowie, wenn die Information verfügbar ist, den Zustellungsstand der Postsendung,
   2. wenn die Anbieterin von Postdiensten Daten registriert und sie nach Abschluss der von einer Kundin oder eines Kunden verlangten Dienstleistung aufbewahrt: sämtliche verfügbaren Daten;
d. die weiteren Auskünfte über den Postverkehr einer Person, die in der Überwachungsanordnung festgehalten sind.

Art. 13 Durchführung der Überwachung

1 Der Dienst bestimmt im Einzelfall, wenn nötig nach Absprache mit der anordnen- den Behörde, die technischen und organisatorischen Massnahmen für die Durchführung der Überwachung.

2 Jede Anbieterin von Postdiensten meldet dem Dienst die Ausführung der

angeordneten Massnahmen.

3 Ist eine Anbieterin von Postdiensten infolge betrieblicher Probleme vorübergehend nicht in der Lage, ihre Pflichten bei einer aktiven Überwachung oder zum Vollzug einer neuen Überwachungsanordnung wahrzunehmen, muss sie dies dem Dienst unverzüglich melden.

4 Der Dienst prüft mit der Anbieterin von Postdiensten, ob Begehren über weitere Auskünfte über den Postverkehr einer Person erfüllt werden können und ob die verlangten Verkehrs- und Rechnungsdaten vorhanden sind. Er benachrichtigt die anordnende Behörde über seine Feststellungen und berät sie, wenn nötig, über das weitere Vorgehen.

Art. 14 Pflichten der Anbieterinnen von Postdiensten

1 Jede Anbieterin von Postdiensten muss in der Lage sein, jene Überwachungstypen nach Artikel 12 auszuführen, die durch sie angebotene Dienste betreffen.

2 Jede Anbieterin von Postdiensten muss in der Lage sein, die Überwachungsanordnungen auch ausserhalb der Dienstzeit entgegenzunehmen und sie so rasch wie möglich auszuführen. Sie meldet dem Dienst den Namen der Kontaktpersonen.

4. Abschnitt: Überwachung des Fernmeldeverkehrs mit Ausnahme von Internet

Technik-asut: Die Abgrenzung des Fernmeldeverkehrs vom Internetverkehr ist nach wie vor unklar, Internet Technologie (damit ist eine Protokollarchitektur gemeint) kann ausserhalb des Internet eingesetzt werden beispielsweise in einen Carrier Class IP Netz (z.B. für VoIP). Damit kann derselbe Dienst (funktionell gesehen) angeboten werden ohne jeglichen Informationstransport über das Internet, unter breitem Einsatz des Internet, oder als Mischform. Sollten sich aus einer Deklaration „Fernmeldedienst-Anbieterin“ vs. „Internet-Anbieterin“ unterschiedlich Verpflichtungen ergeben, besteht die Gefahr von ungleichen Behandlungen verschiedener Provider.

Art. 15 Überwachungsanordnung

1 Die beim Dienst eingereichte Überwachungsanordnung muss die folgenden Angaben enthalten:

a. den Namen der anordnenden Behörde;
b. den Namen der Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist;

c. soweit diese Daten bekannt sind: die Namen, Adressen und Berufe der tat- verdächtigen Personen und der allenfalls zu überwachenden weiteren Personen;
d. im Fall von Personen, die einem Berufsgeheimnis nach Artikel 271 Absatz 1 der Strafprozessordnung3 (StPO) unterstehen: einen Vermerk über diese Besonderheit;
e. die Straftat, die mit der Überwachung aufgeklärt werden soll;
f. wenn möglich, den Namen der Anbieterin von Fernmeldediensten;
g. die angeordneten Überwachungstypen;
h. die bekannten Adressierungselemente;
i. wenn nötig, die Anträge:
   1. auf die Bewilligung einer Direktschaltung,
   2. auf die allgemeine Genehmigung für die Überwachung von mehreren Anschlüssen ohne Genehmigung im Einzelfall (Artikel 272 Absätze 2 und 3 StPO)[4] , und 3. auf die zusätzlichen Vorkehren zum Schutz der Persönlichkeit;
j. den Beginn und die Dauer der Überwachung;
k. die vom Dienst gewünschten Zusatzaufgaben gemäss Artikel 13 Absatz 2 BÜPF.

2 Wenn die Durchführung gewisser Überwachungstypen es erfordert, kann das Departement vorsehen, dass die dem Dienst eingereichte Überwachungsanordnung weitere technische Angaben enthalten soll.

Art. 16 Überwachungstypen (Echtzeit und rückwirkend)
Folgende Überwachungstypen können angeordnet werden:

a. die Übertragung des Fernmeldeverkehrs (Echtzeit-Überwachung der Nutz-informationen);
b. bei Mobiltelefonie: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne , mit der das Endgerät der überwachten Person momentan verbunden ist (Echtzeit-Überwachung);

Technik-asut: Dieser Fall bezieht sich auf einen dauernden Locationupdate, auch wenn weder eine erfolgreiche Kommunikation noch ein erfolgloser Versuch (z.B. Besetzt) zu Stande kommt.

c. die Bereitstellung und die simultane oder periodische Übertragung folgender Angaben , selbst wenn es nicht zum Aufbau einer Kommunikation kommt, (Echtzeit-Überwachung):
   1. die verfügbaren Adressierungselemente (Rufnummern der

abgehenden und ankommenden Kommunikationsvorgänge),
2. die tatsächliche bekannte Zielrufnummer und die zwischengeschalteten verfügbaren Rufnummern, falls der Anruf um- oder weitergeleitet wurde,
3. die erzeugten Signale, einschliesslich der Zeichengabe für den Bereitschaftszustand, die Parameter der Fernmeldeanlagen (z. B. SIM-Nummer, IMSI-Nummer, IMEI-Nummer) und die erzeugten Signale für die Aktivierung von Konferenzschaltung oder Anrufumleitung,
4. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne , mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,
5. das Datum, die Zeit und die Dauer der Verbindung;

Technik-asut: Bei Echtzeitüberwachung sind die Parameter gemäss 5. durch Time Stamps gegeben.

d. die Lieferung folgender Daten, wenn es zum Aufbau einer Kommunikation gekommen ist (rückwirkende Überwachung):
   1. die verfügbaren Adressierungselemente (Rufnummern der abgehenden und eingehenden Kommunikationsvorgänge, sofern diese der Fernmeldedienstanbieterin bekannt sind),
   2. die Kommunikationsparameter des Endgerätes der Mobiltelefonie und die Parameter zur Teilnehmeridentifikation (wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer),

Technik-asut: Unter der Anwendung der Terminologie gemäss ETSI TS 102 657 bezieht sich Art. 16 Bst. d. auf „Verkehrsdaten“ (→ Usage), für Telefonie sind die Parameter definiert in ETSI TS 102 657 Annex B.3, set telephonyServiceUsage.
Da die Abgrenzung Fernmeldedienst zu Internet nicht klar ist, bleibt offen, welche andern Annexes Anwendung finden.

Gemäss „Begriffe und Abkürzungen“ 9. besteht folgende Definition: Kommunikationsparameter: die Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind (Art. 3 Bst. g FMG);
Gemäss dieser Definition sind SIM-Nummer (was ist wirklich damit gemeint; Seriennummer des SIM? In ETSI TS 102 657 ist die SIM-Nummer

nicht definiert), IMSI, MSISDN Parameter, die mit dem Kunden assoziiert sind und der Identifikation der Person dienen und sind „Parameter zur Teilnehmeridentifikation“. Die IMEI ist mit einem Mobiledevice assoziiert und ist ein „Kommunikationsparameter des Endgerätes der Mobiltelefonie“.
In 2. ist keine klare Zuteilung der Parameter in Klassen gegeben; IMEI sei als „Kommunikationsparameter des Endgerätes“ und IMSI als „Parameter zur Teilnehmeridentifikation“ auszuweisen. Zudem erzeugen Formulierung „(wie die SIM-Nummer, die IMSI-Nummer und die IMEI-Nummer)“ Rechtsunsicherheit, da nicht festgelegt ist, was auch noch gemeint sein könnte.
In jedem Fall ist aus der Sicht Technik in ETSI TS 102 657 die vollständige Liste der Parameter enthalten, die unter Vorbehalt einer gesetzlichen Grundlage gefordert werden können.

Die Definition des „ Kommunikationsparameter“ gemäss FMG hat eine enge Verwandtschaft zu der Definition gemäss ITU-T Recommendation Y.2091:
13.1 identifier: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3. bei Mobiltelefonie: den Zell-Identifikator (Cell ID), den Standort und die Hauptstrahlungsrichtung der Antenne , mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist,
4. das Datum, die Zeit und die Dauer der Verbindung

e. der Antennensuchlauf: zur rückwirkenden Eruierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge während eines bestimmten Zeitraumes, wenn es zum Aufbau einer Kommunikation gekommen ist.

Art.16a Suche und Rettung vermisster Personen

Für die Suche und Rettung vermisster Personen gemäss Artikel 3 BÜPF 5 können nur die folgenden Überwachungstypen angeordnet werden

a. die Überwachungstypen nach Artikel 16 Buchstaben b, c und d,

b. soweit möglich die Bestimmung der letzten aktiven Position des mobilen Endgerätes der vermissten Person und die Lieferung aller zur Standortbestimmung notwendigen Angaben, wie:
   1. Zell-Identifikator (Cell ID),
   2. Standort,
   3. Hauptstrahlungsrichtung und Frequenzband der Antenne der Mobiltelefonie.

Art. 16b Überwachungsmassnahmen mit Auslandsbezug

1 Ziel der Überwachungsmassnahmen nach Artikel 16 Buchstabe a, Buchstabe c Ziffern 1, 2, 3 und 5 und Buchstabe d Ziffern 1, 2 und 4 kann jedes Adressierungselement sein, unabhängig vom Standort des Endgeräts, von der Landeskennzahl der Rufnummer und von der Netzzugehörigkeit.

2 Ziel der Überwachungsmassnahmen nach Artikel 16 Buchstabe a, Buchstabe b, Buchstabe c Ziffer 4 und Buchstabe d Ziffer 3 und nach Artikel 16a kann auch ein ausländisches Adressierungselement sein, welches sich im Netzwerk einer schweizerischen Fernmeldedienstanbieterin befindet.

Technik-asut: Es muss klargestellt werden, dass bezugnehmend auf Art. 16 Bst. c. nur jene Parameter ermittelbar sind, die den Gateway in Form von Signalisierung passieren, mit einigen Vorbehalten bezüglich der Verifikation derer Richtigkeit. Der Bezug zu Artikeln aus der Überwachung eines Telefondienstes vermittelt den falschen Eindruck, bei einer Kopfschaltung liesse sich derselbe Umfang an Parametern ermitteln. Die Methode Anforderungen gemäss Art. 16 auf die Kopfschaltung zu übertragen ist ungeeignet und schafft Rechtsunsicherheit.

Technik-asut: Betreffend Anwendung von Art. 16 Bst. d. (rückwirkende Überwachung) ist zu berücksichtigen dass vom Target in der Regel, weil nicht Kunde des verpflichteten Providers (Ausnahmen sind outbound Roamer und inbound Roamer) kein Datensatz existieren kann, der mit einer Subscription assoziiert ist. Es ist nicht zumutbar, dass ein Provider eine Art „virtuelle Accounts“ kreiert und die gesamte Kommunikation von Targets mit Auslandsbezug analysiert und durch Korrelation der vielfältigen sogenannten Kommunikationsparameter einem „virtuellen Account“ zuordnen muss; dies würde eine Data Retention im Bereich „Usage“ für alle inbound und outbound Verbindungen bedingen.
Auch in diem Fall ist die Methode Anforderungen gemäss Art. 16 auf die Kopfschaltung zu übertragen ungeeignet und schafft Rechtsunsicherheit.

Technik-asut: Gemäss „Begriffe und Abkürzungen“ bestehen folgende Definitionen:
8. Adressierungselemente: Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern (Art. 3 Bst. f des Fernmeldegesetzes vom 30. April 1997 9 - FMG); Die Target Identity ist beschränkt auf ein Nummerierungselement → „Adressierungselement“ sei zu ersetzen durch „Nummerierungselement“.

Hier besteht ein gewisses Terminologieproblem zu der Definition gemäss ITU-T Recommendation Y.2091:
13.3 address: An address is the identifier for a specific termination point and is used for routing to this termination point.
Gemäss ITU-T ist eine Address ein Identifier, der einem bestimmten Zweck dient, womit Identifier hierarchisch über der Address steht (d.h. ein Identifier kann eine Address sein, muss es jedoch nicht). Die von BAKOM im FMG niedergeschriebene Hierarchie steht zu jener von ITU-T im Widerspruch.

Art. 17 Durchführung der Überwachung

1 Der Dienst bestimmt im Einzelfall, wenn nötig nach Absprache mit der anordnen- den Behörde, die technischen und organisatorischen Massnahmen für die Durchführung der Überwachung.

2 Wenn der Dienst feststellt, dass die angeordnete Überwachung den Anschluss von Trägerinnen und Trägern von Berufsgeheimnissen betrifft, ohne dass Vorkehren nach Artikel 271 Absatz 1 der Strafprozessordnung6 (StPO) angeordnet worden sind, so zeichnet der Dienst den Fernmeldeverkehr auf und benachrichtigt die Genehmigungsbehörde.

3 Jede Anbieterin von Fernmeldediensten meldet dem Dienst die Ausführung der angeordneten Massnahmen.

4 Sie leitet dem Dienst auf Verlangen die Daten zu . Der Dienst regelt in seinen Richtlinien nach Anhörung der Anbieterinnen die Spezifikationen dieser Zuleitung unter Berücksichtigung der Standards des Europäischen Institutes für Telekommunikationsnormen (ETSI).

Technik-asut: Es ist unklar was alles mit „Zuleitung“ gemeint ist.
ETSI spezifiziert die Auslieferungsformate an einem Übergabeinterface (Handover Interface, HI), spezifiziert jedoch die Ausleitungsnetze (Delivery Networks) aus der Infrastruktur des Providers (IIF/MD) zur Infrastruktur von ÜPF (LEMF) nur oberflächlich. Wenn „die Spezifikationen dieser Zuleitung“ bedeuten würde, dass ÜPF Delivery Networks spezifiziert, würde dies einen erheblichen Eingriff in die Netzhoheit der Provider bedeuten.

5 Bei Überwachungsmassnahmen, die nicht explizit in dieser Verordnung aufgeführt sind, stellt sie dem Dienst jene Schnittstellen zur Verfügung, von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann. Der Dienst regelt die Überwachungsmodalitäten im Einzelfall.

Technik-asut: Eine Schnittstelle ist ein Übergabepunkt zwischen Entitäten, im vorliegenden Fall zwischen Ausrüstungen der Provider und solchen von ÜPF. Damit ein Provider solche Schnittstellen zur Verfügung stellen kann, müssen diese in Technischen Richtlinien spezifiziert sein (mit Ausnahme eines passiven Arrangements zur Auskopplung von Daten, wie TAP).
Der Wortlaut „von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann“ lässt darauf schliessen, dass ÜPF mit eigenen Ausrüstungen an Standorten der Provider ist.
Eine der Kernfragen in diesem Zusammenhang ist die Definition des Spezialfalles.
In den Erläuterungen Site 2 steht:
Der Dienst und die Fernmeldedienstanbieterinnen sind nach dieser Auffassung daher auch verpflichtet, angeordnete und genehmigte Überwachungsmassnahmen durchzuführen, die nicht explizit in der VÜPF aufgeführt sind. Diese Situation führt zu einer grossen Rechtsunsicherheit und dazu, dass sowohl auf Seiten des Dienstes als auch auf Seiten der Fernmeldedienstanbieterinnen bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmassnahmen erhebliche Kosten entstehen. Die Durchführung von diesen Spezialmassnahmen, z. B. im Bereich der Internetüberwachung, kann Kosten für die Anschaffung von Überwachungstechnologie und Supportleistungen sowie den Beibezug von externen Spezialisten in Höhe von mehreren hunderttausend Franken pro Fall verursachen, welche bisher durch den Dienst getragen werden mussten.
Für die Kosten der Provider ist nicht massgebend, ob eine Massnahme in VÜPF definiert ist, sondern ob eine Technische Richtlinie besteht, die es einem Provider gestattet, jene technischen Vorkehrungen zu treffen, die eine kostengünstige Überwachung erlauben. Die Technische Richtlinien sind auch notwendig, damit ÜPF eigne Ausrüstungen beschaffen kann, um die Daten entgegennehmen zu können.
Damit müssten Technische Richtlinien erarbeitet werden für Massnahmen die im VÜPF nicht vorgesehen sind.

6 Ist infolge technischer oder anderer Pannen eine Anbieterin von Fernmeldediensten vorübergehend nicht in der Lage, ihre Pflichten bei aktiven Überwachungen oder zum Vollzug neuer Überwachungsanordnungen wahrzunehmen, muss sie dies dem Dienst unverzüglich mitteilen. Die Verkehrsdaten, welche nicht dem Dienst übertragen werden konnten, sind nachzuliefern.

Technik-asut: In der Praxis hat sich gezeigt, dass hier Interpretationsspielraum in der „Schuldfrage“ besteht. Die sogenannte Panne kann verursacht werden durch Probleme im Bereich der Datenaufbereitung ein verpflichteten Provider, im Delivery Network, bei Ausrüstungen der Behörden, die den ausgeleiteten Verkehr nicht entgegennehmen können. Die Lösung des Problems bedingt die Definition von Übergabeputen, siehe Kommentar zu Art.9 Abs. 2

7 Die Überwachung ist so durchzuführen, dass weder die überwachte Person noch andere Teilnehmerinnen und Teilnehmer davon Kenntnis erhalten. Sie ist so zu planen, dass eine unbefugte oder unsachgemässe Verwendung der erfassten Informationen verhindert wird.

Art. 18 Pflichten der Anbieterinnen von Fernmeldediensten

1 Jede Anbieterin von Fernmeldediensten muss in der Lage sein, die Überwachungstypen nach Artikel 16 auszuführen, die durch sie angebotene Dienste betreffen.

2 Die Überwachung des Fernmeldeverkehrs ist von der Aufnahme des Kundenbetriebes eines Fernmeldedienstes an sicherzustellen.

3 Jede Anbieterin von Fernmeldediensten muss sicherstellen, dass sie die Überwachungsanordnungen ausserhalb der Dienstzeit entgegennehmen und sie so rasch wie möglich ausführen kann. Sie meldet dem Dienst schriftlich die Kontaktangaben der verantwortlichen Personen .4 Sie muss eine durch den Dienst im Verhältnis der Zahl ihrer Teilnehmerinnen und Teilnehmer festgelegte Anzahl Anschlüsse gleichzeitig überwachen können.

5 Sie hat zu gewährleisten, dass innerhalb des durch die Überwachungsanordnung bestimmten Zeitraumes die Überwachung des gesamten über ihre eigene Infrastruktur geführten Fernmeldeverkehrs ermöglicht wird:

a. wenn er über den überwachten Anschluss abgewickelt wird;
b. wenn er zu technischen Speichereinrichtungen unter Kontrolle der eigenen Infrastruktur geleitet wird; oder
c. wenn er aus solchen abgerufen wird.

6 Der Dienst kann die Anbieterinnen von Fernmeldediensten zur Zusammenarbeit verpflichten, um die Überwachung des Fernmeldeverkehrs zu vollziehen, der zwischen verschiedenen Netzen übermittelt wird oder von verschiedenen Anbieterinnen verarbeitet wird.

7 Zur Überprüfung der Überwachungsbereitschaft haben die Anbieterinnen von Fernmeldediensten dem Dienst die Benutzung ihrer Fernmeldedienste unentgeltlich zu gewähren.

Technik-asut: Hier geht es um das sogenannte „permanent Testing Environment“, in dem permanent Testtargets angelegt auf Abbos der Behörden eingerichtet sind. Es ist nicht klar, wessen „Überwachungsbereitschaft“ überprüft werden soll; dies hat einen Einfluss auf den Umfang „permanent Testing Environment“. Es ist auch nicht klar, welche Testmethode eingesetzt werden soll (periodisch vs. bei Unregelmässigkeiten) ; dies hat einen Einfluss auf den Verkehr, den die Provider gratis abzuwickeln haben, gegebenenfalls ins Ausland.

8 Wenn nötig, unterstützen die Anbieterinnen von Fernmeldediensten den Dienst, um sicherzustellen, dass die übermittelten Überwachungsdaten tatsächlich mit dem Fernmeldeverkehr der überwachten Personen übereinstimmen .

Technik-asut: Dies könnte bedeuten, dass die Provider zwecks späterer Verifikation Kopien von abgelieferten Daten erstellen müssten. Es ist unklar, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um diese Unterstützung zu leisten.

5. Abschnitt: Auskünfte über Fernmeldeanschlüsse mit Ausnahme von Internet

Art. 19 System zur Vermittlung der Auskunftsgesuche über die Fernmeldeanschlüsse

1 Der Dienst erstellt und führt in Zusammenarbeit mit den Anbieterinnen von Fernmeldediensten ein System, das die Auskunftsgesuche über die Fernmeldeanschlüsse vermittelt und folgende Auskünfte gibt (Vermittlungssystem):

a. die Adressierungselemente der Anschlüsse einer bestimmten Person;
b. soweit verfügbar, die Identität der Personen, deren Anschlüsse mit bestimmten Adressierungselementen übereinstimmen.

Technik-asut: Hier handelt es sich um Daten, die durch das Call Center Information System (CCIS) erhoben werden. Dies entspricht in der Data Retention gemäss ETSI TS 102 657 den Formaten in Annex A.3.3 GenericSubscriberInfo sowie Annexes B.3,, C.3, D.1, E3 <service>Subscriber .

2 Das Vermittlungssystem sucht den Namen der Anbieterin von Fernmeldediensten und die Angaben nach Artikel 14 Absatz 1 BÜPF:

a. durch den automatisierten Abruf des Verzeichnisses der Fernmeldeanschlüsse der Anbieterin von Fernmeldediensten; oder
b. durch die Weiterleitung des Auskunftsgesuches an die Anbieterin von Fernmeldediensten.

3 Die Anbieterinnen von Fernmeldediensten müssen die Auskunftsgesuche innert der Frist beantworten, die das Departement für die betreffende Dringlichkeitsstufe festlegt.

4 Die Anbieterinnen von Fernmeldediensten müssen die Informationen nach Absatz 1 laufend nachführen. Nach Ausschalten eines Anschlusses müssen die diesbezüglichen Daten noch während sechs Monaten zur Auskunftserteilung zur Verfügung stehen.

5 Die Anbieterinnen von Fernmeldediensten übernehmen die Kosten der Infrastruktur, die sie für die Behandlung der Auskunftsgesuche brauchen; der Dienst über- nimmt die Installations- und Betriebskosten für das Vermittlungssystem.

Art. 19*a*[8] Erfassung von Personendaten beim Verkauf von Prepaid-SIM-Karten

Die Anbieterinnen von Fernmeldediensten müssen sicherstellen, dass beim Verkauf von Prepaid-SIM-Karten die Personalien der Kundinnen und Kunden (Name, Vorname, Adresse, Geburtsdatum) anhand eines gültigen Reisepasses, einer Identitätskarte oder eines anderen für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes erfasst werden. Ausserdem sind die Art des Ausweises und die Ausweisnummer zu erfassen.

Art. 20 Benützung des Vermittlungssystems

1 Jede in Artikel 14 Absatz 2 BÜPF erwähnte Behörde bezeichnet die Personen, die für die Benutzung des Vermittlungssystems vorgesehen sind.

2 Der Dienst erteilt die Zugriffsbewilligungen an diese Personen, wenn eine genügende Benutzungsfrequenz zu erwarten ist:

a. zur Bestimmung der zu überwachenden Anschlüsse und Personen;
b. für die Erfüllung von Polizeiaufgaben;
c. zur Erledigung von Verwaltungsstrafsachen.

Art. 21 Protokollierung

1 Der Dienst protokolliert die Zugriffe auf das Vermittlungssystem.

2 Er bewahrt die Protokolle während eines Jahres auf. Die Protokolle werden so ausgestaltet, dass die abgefragten Daten festgestellt werden können. Er vernichtet sie nach Ablauf der Aufbewahrungsfrist.

3 Die Anbieterinnen von Fernmeldediensten dürfen die Auskunftsgesuche anonymisiert protokollieren.

Art. 22 Auskunftserteilung durch den Dienst

1 Die in Artikel 14 Absatz 2 BÜPF erwähnten Behörden können vom Dienst Auskunft über die Fernmeldeanschlüsse verlangen. Sie reichen ihre Auskunftsbegehren per Post, per Telefax oder mit einem anderen durch das Departement zugelassenen sicheren Übertragungsmittel ein.

2 Der Dienst bewahrt die Auskunftsgesuche und die erteilten Antworten während eines Jahres auf. Er vernichtet diese Daten nach Ablauf der Aufbewahrungsfrist.

6. Abschnitt: Überwachung des Internets

Technik-asut: Es ist unklar, wofür Ausdruck Internet verwendet wird, d.h. für:

a) "The Internet" wobei man behaupten könnte, dass jeder der als "Vernetzer" und/oder Application Service Povider und/oder "Hoster" auftritt, Mitglied der "Internet Community" ist;

b) Ein Netz in IP-Technologie, dessen Kommunikation nie in "The Internet" verlaufen muss, aber bei Nomadisierung in "ferne Länder" in "The Internet" verlaufen kann.

Mit dem Titel "Überwachung des Internet" will offenbar ÜPF "jedermann" verpflichten der IP-Technologie einsetzt, unabhängig davon, ob eine Kommunikation im "eigenen" Netz bleibt oder in "The Internet" verläuft, respektive ob er nur „Application Service Provider“ und/oder „Hoster“ ist. "The Internet" selbst ist eine „unfassbare Wolke“ die zu überwachen schwierig ist; deshalb ist der Ausdruck "Überwachung des Internet"

ungeeignet, eine bestimmte Absicht auszudrücken.

Die Definition im Anhang „Begriffe und Abkürzungen“

1. Internet-Anbieterin: Fernmeldedienstanbieterin oder der Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien (Netzprotokoll im Internet [Internet Protocol]) unter Verwendung von IP-Adressen anbietet;

zeigt eher auf b).

Rahmen des Internet werden folgende Dienstleistungen erbracht:
i) Zugang zu Internet
ii) Application Services wie E-mail
iii) Hosting von Applikationen für Dritte

Art. 23 Überwachungsanordnung

Technik-asut: Der Inhalt ist bezüglich Inhalt und Beschreibungstiefe mit Art.15 Abs. 1 abzugleichen.

Die beim Dienst eingereichte Überwachungsanordnung muss die folgenden Angaben enthalten:

a. den Namen der anordnenden Behörde;
b. den Namen der Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist;
c. soweit diese Daten bekannt sind: die Namen, Adressen und Berufe der tatverdächtigen Personen und der allenfalls zu überwachenden weiteren Personen;
d. im Fall von Personen, die einem Berufsgeheimnis nach Artikel 271 Absatz 1 der Strafprozessordnung7 (StPO) unterstehen: einen Vermerk über diese Besonderheit;
e die Straftat, die mit der Überwachung aufgeklärt werden soll;
f. den Namen der Internet-Anbieterin, wenn sie bekannt ist;
g. die angeordneten Überwachungstypen, einschliesslich :
1. der bekannten Adressierungselemente (E-Mail-, elektronische Postfach- , Rechner- und IP-Adresse, Benutzername, MAC-Adresse, E.164-Nummer, SIP URI, IMSI-Nummer, IMEI-Nummer usw.),

Technik-asut: In Art. 15, Abs. 1, Bst. h. steht: „die bekannten Adressierungselemente;“ ohne Liste.

2. der bekannten Anmeldungsdaten (Log-in),
3. der Bewilligung einer Direktschaltung,
4. der Anträge von zusätzlichen Vorkehren zum Schutz nicht beteiligter Benutzerinnen und Benutzer;

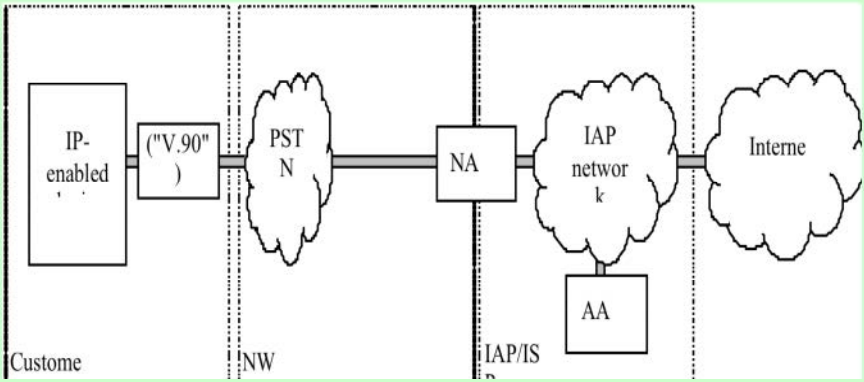
h. den Beginn und das Ende der Überwachung;
i. die vom Dienst gewünschten Zusatzaufgaben gemäss Artikel 13 Absatz 2 BÜPF.

Art. 24 Überwachbare Internetzugänge und Anwendungen

1 Folgende Internetzugänge können überwacht werden:

a. Zugang über eine Telefonverbindung;

Technik-asut: Ein Zugang über eine Telefonverbindung ist ein Arrangement gemäss ETSI TS 102 232-3 § 5.1.1 Dial-up access, siehe Figur 2/TS 102 232-3



Der Accessprovider ist eigentlich der Provider des Network Access Servers (NAS), d.h. der Internet Access Provider (IAP), der auch AAA implementiert, und nicht er Provider des PSTN/ISDN. Für den PSTN/ISDN Provider handelt es sich um eine „normale“ Verbindung, die im Rahmen der „Anwendungsüberwachung“ ausgelenkt wird, allerdings zusammen mit der Kommunikation zwischen Personen. Eine Filterung ist in diesem Fall Angelegenheit der Behörden.
Es ist zu berücksichtigen, dass anstelle des PSTN/ISDN auch ein GSM oder in VoIP Netz eingesetzt werden könnte d.h. jedes Netz, das ein

Modem mit einem Network Access Server (NAS) verbinden kann.

a. sollte geändert werden von „Zugang über eine Telefonverbindung“ auf „Zugang durch eine Wählverbindung zu einem Network Access Server“

Massgebend ist die funktionelle Architektur wie in Figur 2/TS 102 232-3 dargestellt und weniger die Technologie des Netzes für den Zugang zum NAS

b. Breitbandzugang (xDSL, Kabelmodem usw.);
c. Zugang über ein Mobilfunknetz (GSM, GPRS, UMTS, LTE usw.);

Technik-asut: Massgebend ist die angewendete Mobile Packet Date Technologie wie GPRS und weniger „ein Mobilfunknetz“. Mobile Circuit Switched (CS) ist durch a. abgedeckt.
c. sollte geändert werden von „ Zugang über ein Mobilfunknetz (GSM, GPRS, UMTS, LTE usw.) “ auf „Zugang mittels Mobile Packet Data Technologie“

d. kabelloser Zugang (Wi-Fi, Wimax, WLL usw.);
e. andere Zugänge zum Netz via OSI-Schicht 2 (z.B. Ethernet über FTTH-Zugang);
f. andere Zugänge zum Netz via OSI-Schicht 3 (z.B. VPN-Zugang).

Technik-asut: Eine Zugangsüberwachung sei beschränkt auf eine Analyse der Inhalte und deren Auslenkung bis zur höchsten Protokollschicht in der Access Architektur und enthält keine Pflicht zur Filterung und selektiven Ausleitung der Protokolle über dem „Access Layer“.
Es sei folgende Ergänzung „Bei diese Überwachung besteht keine Pflicht einer Filterung und selektiver Ausleitung von Informationsflüssen die durch Elemente über der höchsten Protokollschicht in der Access Architektur identifiziert werden.“

2 Folgende Anwendungen können überwacht werden:
a. synchrone und asynchrone elektronische Postdienste (Instant Messaging, E-Mail usw.);
b. Multimediadienste (VoIP, Audio- und Videoübertragungen usw.).

Art. 24a Überwachungstypen (Echtzeit)
Als Echtzeitüberwachung können folgende Überwachungstypen angeordnet werden:

a. die Übermittlung sämtlicher Daten, die über den überwachten Zugang gesendet oder empfangen werden;

Technik-asut: Mit „sämtlichen“ Daten sind wohl Content of Communication (CC, HI3) und Intercept Related Information (IRI, HI2) im Sinne des ETSI gemeint.

b. die Bereitstellung und die simultane oder periodische Übermittlung der folgenden Auskünfte über den Internetzugang:

Technik-asut: Der Ausdruck „Auskünfte“ hat gegeben durch BÜPF verschiedene Bedeutungen, jedoch in keinem Fall im Zusammenhang mit einer Echtzeitüberwachung:
BÜPF Art. 5 „Auskünfte über den Post- und Fernmeldeverkehr“
BÜPF Art. 14 „ Auskünfte über Fernmeldeanschlüsse“
Der Ausdruck „Auskünfte“ sei zu ersetzen durch „Angaben“ (in Art 24 Bst. d. wird auch der Ausdruck „Angaben“ verendet),

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

Technik-asut: Bei Echtzeitüberwachung sind die Parameter gemäss 1. durch Time Stamps gegeben.

2. die Art der Datenverbindung oder des Anschlusses,
3. die verwendeten Anmeldungsdaten (Log-in),
4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation,
5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (MAC-Adresse, IMEI-Nummer, IMSI-Nummer usw.),

Technik-asut: Es muss eine klare Zuordnung der Parameter in Klassen „Kommunikationsparameter des Endgerätes“ → IMEI und „Parameter zur Teilnehmeridentifikation“ → IMSI geben. Siehe auch Kommentar zu Art. 16 Bst. d.

6. bei Zugang über ein Mobilfunknetz: die Bestimmung und die periodische Übertragung des Zell-Identifikators (Cell ID), des

Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist,

7. die technischen Änderungen, die während der Verbindung stattfinden, und ihre Ursachen, falls bekannt;

Technik-asut: Gemäss den Erläuterungen handelt es sich bei 7. um folgende Situationen: „Diese Ziffer erwähnt die Informationen, die während einer Kommunikationsverbindung verlangt werden können. In diesem Fall hat die Strafverfolgungsbehörde die Möglichkeit, einen technischen Bericht betreffend alle Änderungen zu verlangen, die die überwachte Person oder die Fernmeldedienstanbieterin veranlasst hat. Es handelt sich etwa um Abonnementsänderungen oder um Änderungen am Netzwerk.

7. scheint Bezug zu nehmen auf Änderungen, die ein Kunde über ein Portal an seiner Subcription oder seinen Einstellungen im Netz (irreführend als „Änderungen am Netzwerk“ bezeichnet) vornimmt. Es ist jedoch nicht realistisch anzunehmen, dass eine gleichwertige Änderung durch einen Agenten des Providers (diese Aktion läuft über Managementkanäle) im Rahmen einer Echtzeitüberwachung eines Zuganges erfasst werden kann.

c. die Übermittlung der Nutzinformationen, die über die überwachte Anwendung gesendet oder empfangen werden ;
d. die Bereitstellung und die simultane oder periodische Übermittlung folgender Angaben über die überwachte Anwendung :
   1. das Datum und die Uhrzeit der Kommunikation (Beginn und Ende),

Technik-asut: Bei Echtzeitüberwachung sind die Parameter gemäss 1. durch Time Stamps gegeben.

2. die verfügbaren Adressierungselemente, insbesondere diejenigen des Ursprungs und des Ziels der Kommunikation ,
3. die verwendeten Anmeldungsdaten (Log-in),
4. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen gemäss SMTP-Protokoll,
5. die anderen verfügbaren Kommunikationsparameter,
6. die technischen Änderungen während der Kommunikation und ihre Ursachen, falls bekannt.

Technik-asut: Gemäss den Erläuterungen handelt es sich bei 6. um folgende Situationen: „ Diese Ziffer erwähnt die Informationen, die während einer Kommunikation über einen Internetservice verlangt werden können. In diesem Fall hat die Strafverfolgungsbehörde die Möglichkeit, einen technischen Bericht betreffend alle Änderungen zu verlangen, die die überwachte Person oder die Fernmeldedienstanbieterin veranlasst hat. Es handelt sich etwa um Abonnementständerungen oder um Änderungen am Log-in.

6. scheint Bezug zu nehmen auf Änderungen, die ein Kunde über ein Portal an seiner Subcription oder seinen Securityeinstellungen vornimmt. Es ist jedoch nicht realistisch anzunehmen, dass eine gleichwertige Änderung durch einen Agenten des Providers (diese Aktion läuft über Managementkanäle) im Rahmen einer Echtzeitüberwachung eines Anwendung erfasst werden kann.

Art. 24b Überwachungstypen (rückwirkend)
Als rückwirkende Überwachung können folgende Überwachungstypen angeordnet werden:

a. die Übermittlung der folgenden Angaben über den überwachten Zugang:
   1. das Datum und die Uhrzeit, zu der die Datenverbindung hergestellt und getrennt wurde,
   2. die Art der Datenverbindung oder des Anschlusses,
   3. die verwendeten Anmeldungsdaten (Log-in),
   4. die verfügbaren Adressierungselemente, insbesondere des Ursprungs der Kommunikation,
   5. die Kommunikationsparameter der Endgeräte und die Parameter zur Teilnehmeridentifikation (MAC-Adresse, IMEI-Nummer, IMSI-Nummer usw.),

Technik-asut: Es muss eine klare Zuordnung der Parameter in Klassen „Kommunikationsparameter des Endgerätes“ → IMEI und „Parameter zur Teilnehmeridentifikation“ → IMSI geben. Siehe auch Kommentar zu Art. 16 Bst. d.

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

b. die Übermittlung der folgenden Angaben bei Versand oder Empfang von Meldungen durch einen asynchronen elektronischen Postdienst :
   1. das Datum und die Uhrzeit des Versands oder des Empfangs von Mitteilungen bei der Internet-Anbieterin,
   2. bei der Überwachung von E-Mail-Verkehr: die Umschlaginformationen nach SMTP-Protokoll,
   3. die IP-Adressen der sendenden und empfangenden Fernmeldeanlagen der asynchronen elektronischen Postdienste ,
   4. die anderen verfügbaren Adressierungselemente.

Art. 24c Überwachungsmassnahmen mit Auslandsbezug
Ziel der Überwachungsmassnahmen nach Artikel 24a Buchstaben a und b und 24b Buchstabe a können auch Anschlüsse nach Artikel 24 Absatz 1 Buchstaben c und d sein, die ein ausländisches Adressierungselement haben, welches sich im Netzwerk einer schweizerischen Fernmeldedienstanbieterin befindet.

Technik-asut: Bei einer Accessüberwachung gemäss Art. 24a Bst. a. und b. sowie Art. 24b Bst. a. stellt sich die Frage, welche Parameter die auftraggebenden Behörden einem Provider bekanntgeben, um einen Informationsfluss zu überwachen, der einen Ursprung „irgendwo“ hat und von „irgendwem“ zugeteilte Indikatoren (z.B. IP-Address) verwendet. Es ist insbesondere zu berücksichtigen, dass Indikatoren des Zuganges dynamisch zugeteilt werden können und demzufolge „falsche Targets“ überwacht würden. In keinem Fall ist der verpflichtete Schweizerische Provider der Accessprovider, sondern betreibt allenfalls ein sogenanntes zwischengeschaltetes Transportnetz.

Bezugnehmend auf den Hinweis auf Artikel 24 Absatz 1 Buchstaben c und d sei festgestellt dass in einem Gateway, die am fernen Ende eingesetzte Access Technologie in der Regel nicht erkennen kann, wobei dies für den beabsichtigten Zweck (d.h. der Überwachung der Kommunikation eines Targets mit einem Kunden des verpflichteten Providers) nicht relevant ist.

Da solche Überwachungen in Gateways umgesetzt werden müssen, was schon durch den Ausdruck „Kopfschaltung“ offensichtlich wird, kommt nur eine Überwachung der Anwendung in Frage.

Es muss klargestellt werden, dass bei einer Echtzeit-Überwachung der Anwendung bezugnehmend auf Art. 24a Bst. c. und d. nur jene Parameter

ermittelbar sind, die den Gateway passieren, mit einigen Vorbehalten bezüglich der Verifikation derer Richtigkeit. Der Bezug zu Artikeln (d.h. Art. 24a), die aus der Überwachung eines Telefondienstes abgeleitet wurden vermittelt den falschen Eindruck, bei einer Kopfschaltung liesse sich derselbe Umfang an Parametern ermitteln. Die Methode Anforderungen gemäss Art. 24a auf die Kopfschaltung zu übertragen ist ungeeignet und schafft Rechtsunsicherheit.

Betreffend Anwendung von Art. 24b Bst. b. (rückwirkende Überwachung) ist zu berücksichtigen dass vom Target in der Regel, weil nicht Kunde des verpflichteten Providers (Ausnahmen sind outbound Roamer und inbound Roamer) kein Datensatz existieren kann, der mit einer Subscription assoziiert ist. Es ist nicht zumutbar, dass ein Provider eine Art „virtuelle Accounts“ kreiert und die gesamte Kommunikation von Targets mit Auslandsbezug analysiert und durch Korrelation der vielfältigen sogenannten Kommunikationsparameter einem „virtuellen Account“ zuordnen muss; dies würde eine Data Retention im Bereich „Usage“ für alle inbound und outbound Verbindungen bedingen.
Auch in dem Fall ist die Methode Anforderungen gemäss Art. 24b auf die Kopfschaltung zu übertragen ungeeignet und schafft Rechtsunsicherheit.

Art. 25 Durchführung der Überwachung

1 Der Dienst bestimmt im Einzelfall:

a. die technischen und organisatorischen Massnahmen für die Durchführung der Überwachung, wenn nötig im Einvernehmen mit der anordnenden Behörde;
b. die zu verwendenden Datenträger, die Art und Weise der Übermittelung und die zulässigen Datenformate, wenn nötig nach Anhörung der Internet-Anbieterin.

2 Wenn der Dienst feststellt, dass die angeordnete Überwachung Trägerinnen und Träger von Berufsgeheimnissen betrifft, ohne dass Vorkehren nach Artikel 271 Absatz 1 der Strafprozessordnung8 (StPO) angeordnet worden sind, zeichnet der Dienst die Daten auf und benachrichtigt die Genehmigungsbehörde.

3 Die Internet-Anbieterinnen melden dem Dienst die Ausführung der angeordneten Massnahmen.

4 Sie leiten dem Dienst auf Verlangen die Daten zu. Der Dienst regelt in seinen Richtlinien nach Anhörung der Anbieterinnen die Spezifikation dieser Zuleitung unter Berücksichtigung der Standards des Europäischen Institutes für Telekommunikationsnormen (ETSI).

Technik-asut: Es ist unklar was alles mit „Zuleitung“ gemeint ist.
ETSI spezifiziert die Auslieferungsformate an einem Übergabeinterface (Handover Interface, HI), spezifiziert jedoch die Ausleitungsnetze (Delivery Networks) aus der Infrastruktur des Providers (IIF/MD) zur Infrastruktur von ÜPF (LEMF) nur oberflächlich. Wenn „die Spezifikationen dieser Zuleitung“ bedeuten würde, dass ÜPF Delivery Networks spezifiziert, würde dies einen erheblichen Eingriff in die Netzhoheit der Provider bedeuten.

5 Bei Überwachungsmassnahmen, die nicht explizit in dieser Verordnung aufgeführt sind, stellen sie dem Dienst jene Schnittstellen zur Verfügung, von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann. Der Dienst regelt die Überwachungsmodalitäten im Einzelfall.

Technik-asut: Eine Schnittstelle ist ein Übergabepunkt zwischen Entitäten, im vorliegenden Fall zwischen Ausrüstungen der Provider und solchen von ÜPF. Damit ein Provider solche Schnittstellen zur Verfügung stellen kann, müssen diese in Technischen Richtlinien spezifiziert sein (mit Ausnahme eines passiven Arrangements zur Auskopplung von Daten, wie TAP).
Der Wortlaut „von denen aus der Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen werden kann“ lässt darauf schliessen, dass ÜPF mit eigenen Ausrüstungen an Standorten der Provider ist.
Eine der Kernfragen in diesem Zusammenhang ist die Definition des Spezialfalles.
In den Erläuterungen Site 2 steht:
Der Dienst und die Fernmeldedienstanbieterinnen sind nach dieser Auffassung daher auch verpflichtet, angeordnete und genehmigte Überwachungsmassnahmen durchzuführen, die nicht explizit in der VÜPF aufgeführt sind. Diese Situation führt zu einer grossen Rechtsunsicherheit und dazu, dass sowohl auf Seiten des Dienstes als auch auf Seiten der Fernmeldedienstanbieterinnen bei der Durchführung von nicht explizit in der VÜPF aufgeführten Überwachungsmassnahmen erhebliche Kosten entstehen. Die Durchführung von diesen Spezialmassnahmen, z. B. im Bereich der Internetüberwachung, kann Kosten für die Anschaffung von Überwachungstechnologie und Supportleistungen sowie den Beibezug von externen Spezialisten in Höhe von mehreren hunderttausend Franken pro Fall verursachen, welche bisher durch den Dienst getragen werden mussten.
Für die Kosten der Provider ist nicht massgebend, ob eine Massnahme in VÜPF definiert ist, sondern ob eine Technische Richtlinie besteht, die es

einem Provider gestattet, jene technischen Vorkehrungen zu treffen, die eine kostengünstige Überwachung erlauben. Die Technische Richtlinien sind auch notwendig, damit ÜPF eigne Ausrüstungen beschaffen kann, um die Daten entgegennehmen zu können.
Damit müssten Technische Richtlinien erarbeitet werden für Massnahmen die im VÜPF nicht vorgesehen sind.

6 Ist infolge technischer oder anderer Pannen eine Internet-Anbieterin vorübergehend nicht in der Lage, ihre Pflichten bei Echtzeit-Überwachungen oder zum Vollzug neuer Überwachungsanordnungen wahrzunehmen, muss sie es dem Dienst unverzüglich mitteilen. Die Verkehrsdaten, welche nicht dem Dienst übertragen werden konnten, sind nachzuliefern.

Technik-asut: In der Praxis hat sich gezeigt, dass hier Interpretationsspielraum in der „Schuldfrage“ besteht. Die sogenannte Panne kann verursacht werden durch Probleme im Bereich der Datenaufbereitung ein verpflichteten Provider, im Delivery Network, bei Ausrüstungen der Behörden, die den ausgeleiteten Verkehr nicht entgegennehmen können.
Die Lösung des Problems bedingt die Definition von Übergabeputen, siehe Kommentar zu Art.9 Abs. 2

7 Die Überwachung ist so durchzuführen, dass weder die überwachte Person noch andere Teilnehmerinnen und Teilnehmer davon Kenntnis erhalten. Sie ist so zu planen, dass eine unbefugte oder unsachgemässe Verwendung der erfassten Informationen verhindert wird.

Art. 26 Pflichten der Internet-Anbieterinnen

1 Jede Internet-Anbieterin muss in der Lage sein, die Überwachungstypen nach diesem Abschnitt auszuführen, die durch sie angebotene Dienste betreffen.

2 Die Überwachung des Fernmeldeverkehrs ist von der Aufnahme des Kundenbetriebes eines Internet-Dienstes an sicherzustellen.

3 Jede Internet-Anbieterin muss sicherstellen, dass sie die Überwachungsanordnungen auch ausserhalb ihrer Bürozeiten empfangen und so rasch wie möglich ausführen kann. Sie meldet dem Dienst schriftlich die Kontaktangaben der verantwortlichen Personen.

4 Sie hat zu gewährleisten, dass innerhalb des durch die Überwachungsanordnung bestimmten Zeitraumes die Überwachung des gesamten über ihre eigene Infrastruktur geführten und den

Überwachungen gemäss Artikel 24 - 24 unterliegenden Internetverkehrs ermöglicht wird, der von der Überwachungsanordnung erfasst ist.

5 Der Dienst kann die Internet-Anbieterinnen zur Zusammenarbeit verpflichten, um die Überwachung des Fernmeldeverkehrs zu vollziehen, der durch mehr als ein Netzwerk führt.

Technik-asut: Es wird zu einer echten Herausforderung für ÜPF werden, die beteiligten Provider zu ermitteln, Grundlage dazu wäre eine funktionelle Architektur und ein Rollenmodell.

6 Zur Überprüfung der Überwachungsbereitschaft haben die Internet-Anbieterinnen dem Dienst die Benutzung ihrer Dienste unentgeltlich zu gewähren.

Technik-asut: Hier geht es um das sogenannte „permanent Testing Environment“, in dem permanent Testtargets angelegt auf Abbos der Behörden eingerichtet sind. Es ist nicht klar, wessen „Überwachungsbereitschaft“ überprüft werden soll; dies hat einen Einfluss auf den Umfang „permanent Testing Environment“. Es ist auch nicht klar, welche Testmethode eingesetzt werden soll (periodisch vs. bei Unregelmässigkeiten) ; dies hat einen Einfluss auf den Verkehr, den die Provider gratis abzuwickeln haben, gegebenenfalls ins Ausland.

7 Wenn nötig, unterstützen die Internet-Anbieterinnen den Dienst, um sicherzustellen, dass die übermittelten Überwachungsdaten tatsächlich mit dem Fernmeldeverkehr der überwachten Personen übereinstimmen.

Technik-asut: Dies könnte bedeuten, dass die Provider zwecks späterer Verifikation Kopien von abgelieferten Daten erstellen müsste. Es ist unklar, welche technischen und organisatorischen Vorkehrungen ein Provider treffen muss, um diese Unterstützung zu leisten.

Art. 27 Auskünfte über Internet-Teilnehmerinnen und -Teilnehmer

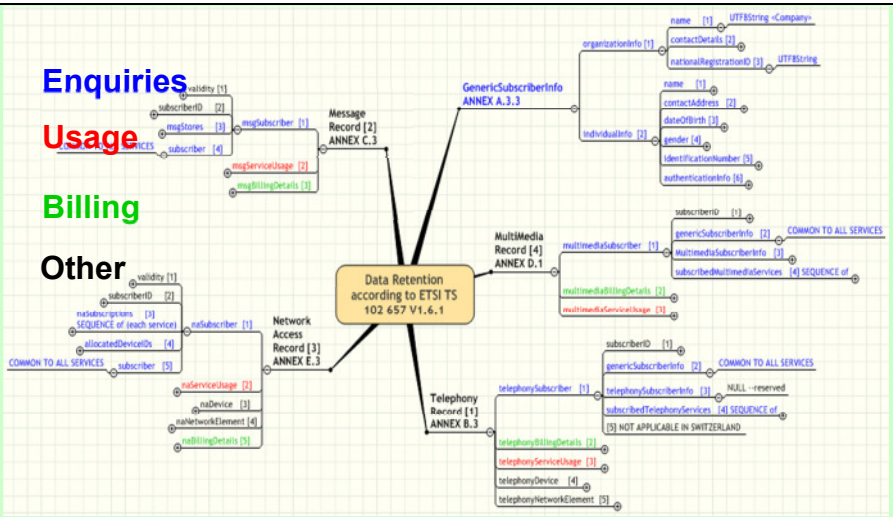
1 Die zuständige Internet-Anbieterin meldet dem Dienst auf Anfrage folgende
Daten:

Technik-asut: Hier handelt es sich um Daten, die gegeben durch ihre Charakteristik im Prinzip durch das Call Center Information System (CCIS) erhoben werden müssten. Dies entspricht in der Data Retention gemäss ETSI TS 102 657 den Formaten in Annex A.3.3 GenericSubscriberInfo sowie Annexes C.3, D.1, E.3 <service>Subscriber .

a. bei IP-Adressen: die Art des Anschlusses, das Datum und die Uhrzeit der Zuteilung oder das Datum und die Uhrzeit des Anfanges und gegebenenfalls des Endes des Zuteilungszeitraumes , den Namen, die Adresse, die Anmeldungsdaten (Log-in) und, soweit bekannt, den Beruf der Teilnehmerin oder des Teilnehmers, sowie weitere IP-Adressen, die die Internet-Anbieterin dieser oder diesem zugeteilt hat;

Technik-asut: In diesem Fall geht es um Auskünfte im Sinn von BÜPF Art. 14 „ Auskünfte über Fernmeldeanschlüsse“.
Diese Auskünfte sind beschränkt auf Personalien, respektive gleichwertige Daten von Unternehmen sowie deren „Subscriptions“ und decken niemals Parameter ab, die durch Interaktionen zwischen einem Kunden und dem Netz erworben werden, wie beispielsweise eine dynamische IP-Adresse mittels DHCP.

Da gemäss Art. 17 Abs. 4 ETSI –Standards berücksichtigt werden sollen, sollte die Klassenbildung von Parametern gemäss ESI TS 102 657 übernommen werden.
Es handelt sich dabei um die blauen Bereiche in der untenstehenden Figur:



Sollte VÜPF von der Klassenbildung gemäss ETSI abweichen, wird eine technische Umsetzung von VÜPF interpretierbar und es besteht die Gefahr von unnötigen rechtlichen Auseinandersetzungen.

BÜPF Art. 5 „Auskünfte über den Post- und Fernmeldeverkehr“ bezieht sich in Abs. 1 auf „Usage“ und „Billing“. Die bezüglich „Usage“ zu erfüllenden Anforderungen sind bereits in Art. 24b definiert.
Die Erweiterung auf alle IP-Adressen und log-in sei zurückzunehmen.

b. bei EDV-Systemen: sofern verfügbar, zusätzlich die Domainnamen und weitere Adressierungselemente unter denen diese der Internet-Anbieterin bekannt sind;
c. bei elektronischen Postdiensten , sofern sie von den Internet-Anbieterinnen zur Nutzung durch Kunden eingerichtet sind: soweit bekannt , den Namen, die Adresse und den Beruf der Teilnehmerin oder des Teilnehmers.

2 Der Dienst sucht über die öffentlich zugänglichen Datenbanken die zuständige Internet-Anbieterin für Auskunftsgesuche und Überwachungen der Internet- Zugänge.

3 Er bewahrt die Auskunftsgesuche und die erteilten Antworten während eines
Jahres auf. Er vernichtet diese Daten nach Ablauf der Aufbewahrungsfrist.

7. Abschnitt: Überwachung des Verkehrs innerhalb von internen Fernmeldenetzen oder Hauszentralen

Art. 28 Vorbereitung der Überwachung

Wenn die Überwachungsanordnung eine Überwachung des Verkehrs innerhalb eines internen Fernmeldenetzes oder einer Hauszentrale vorsieht, bestimmt der Dienst im Einvernehmen mit der Betreiberin dieses Netzes oder dieser Zentrale und wenn nötig mit der anordnenden Behörde, wie die Überwachung durchzuführen ist.

Art. 29 Durchführung der Überwachung

1 Der Dienst richtet die Überwachung selber ein oder beauftragt damit auf eigene Kosten die Betreiberin des internen Fernmeldenetzes oder der Hauszentrale, wenn diese einverstanden ist und über die angemessenen Einrichtungen verfügt.

2 Wenn die Betreiberin mit der Überwachung beauftragt ist, müssen die Auflagen für die Datensicherheit im Auftrag enthalten sein.

8. Abschnitt: Gebühren und Rechtsschutz

Art. 30 Gebühren und Entschädigungen

1–2 ...[9]

3 Die anordnende Behörde kann vom Dienst verlangen, dass er ihr die zu erwarten- den Kosten für eine bestimmte Überwachung mitteilt.

Art. 31 Rechnungsstellung

1 Der Dienst stellt den anordnenden Behörden nach Abschluss der Überwachung
Rechnung für die gesamten erbrachten Dienstleistungen.

2 Die Anbieterinnen von Post- oder Fernmeldediensten übermitteln dem Dienst ihre
Abrechnungen spätestens zwei Monate nach Abschluss der Überwachung.

Art. 32[10] Rechtsschutz

Gegen Verfügungen des Dienstes über den Vollzug dieser Verordnung kann nach den allgemeinen Bestimmungen über die Bundesrechtspflege Beschwerde geführt werden.

9. Abschnitt: Schlussbestimmungen

Art. 33 Vollzug

1 Das Departement regelt:

a. die zugelassenen Übertragungsmittel zur Einreichung der Überwachungsanordnungen nach Artikel 5 Absatz 1 Buchstabe a;

b. die Fristen für die Beantwortung der Auskunftsgesuche nach Artikel 19 Absatz 3 in Funktion der verschiedenen Dringlichkeitsstufen;

c. die Anforderungen an die Auskunftsgesuche nach den Artikeln 22 und 27;

d. wenn nötig, die technischen ergänzenden Angaben, die in Artikel 15 Absatz 2 erwähnt sind;

e. ...[11]

1bis Der Dienst regelt durch Richtlinien die technischen und administrativen Einzelheiten der einzelnen Überwachungstypen.[12]

9 Aufgehoben durch Art. 7 der V vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR **780.115.1**).

10 Fassung gemäss Ziff. II 77 der V vom 8. Nov. 2006 über die Anpassung von Bundesratsverordnungen an die Totalrevision der Bundesrechtspflege, in Kraft seit 1. Jan. 2007 (AS **2006** 4705).

11 Aufgehoben durch Ziff. I der V vom 12. März 2004 (AS **2004** 1431).

12 Eingefügt durch Ziff. I der V vom 12. März 2004 (AS **2004** 1431).

2 Er legt Form und Inhalt folgender Formulare fest:

a. die durch die anordnende Behörde zu verwendenden Formulare, um die Überwachungsanordnung beim Dienst einzureichen;

b. die durch den Dienst zu verwendenden Formulare, um die Anbieterinnen von Post- oder Fernmeldediensten mit der Durchführung der Überwachungsanordnung zu beauftragen;

c. die durch die Behörden nach Artikel 14 Absatz 2 BÜPF zu verwendenden Formulare, um vom Dienst die Auskünfte nach den Artikeln 22 und 27 einzuholen.

3 Das Departement räumt den Anbieterinnen von Post- und Fernmeldediensten beim Erlass von technischen Vorschriften

angemessene Übergangsfristen für die Umsetzung ein.

Art. 34 Aufhebung bisherigen Rechts

Die Verordnung vom 1. Dezember 1997[13] über den Dienst für die Überwachung des
Post- und Fernmeldeverkehrs wird aufgehoben.

Art. 35 Änderung bisherigen Rechts

Die Verordnung vom 6. Oktober 1997[14] über Fernmeldedienste wird wie folgt geändert:

Art. 50 Abs. 1

...

Art. 36 Übergangsbestimmungen

1 Während maximal drei Monaten nach Inkrafttreten dieser Verordnung vollzieht der Dienst die Überwachungsanordnungen, die nach dem alten Recht genehmigt worden sind.

2 Bis zur Inbetriebnahme des Verarbeitungszentrums nach Artikel 8 übertragen die Anbieterinnen von Fernmeldediensten die Daten aus der Überwachung des Fernmeldeverkehrs nach bisheriger Praxis an den Dienst. Der Dienst zeichnet den Fern- meldeverkehr auf oder überträgt ihn mit Direktschaltung an die Strafverfolgungsbehörde, die als Empfängerin der Überwachungsdaten vorgesehen ist.

3 Die Anbieterinnen von Post- oder Fernmeldediensten melden innert drei Monaten nach Inkrafttreten dieser Verordnung die Überwachungsmassnahmen innerhalb ihres Dienstleistungsangebots, die sie nicht imstande sind auszuführen. Sie treffen die notwendigen Massnahmen, um diese Überwachungstypen innerhalb der durch den Dienst im Einzelfall festgesetzten Frist ausführen zu können und melden es dem Dienst, sobald sie dazu in der Lage sind.

13 [AS **1997** 3022]

14 [AS **1997** 2833, **2000** 1044. AS **2001** 2759 Art. 83]

4 Spätestens vom 1. April 2004 an übertragen die Anbieterinnen von Fernmelde- diensten die Daten aus jeder Überwachung des Fernmeldeverkehrs gemäss den Richtlinien nach Artikel 33 Absatz 1[bis]. Das Departement kann den Gebührenanteil von Anbieterinnen, die diese Daten schon zwischen dem 1. April 2003 und dem
1. April 2004 nach den neuen Anforderungen übertragen, angemessen

erhöhen; die Mehrkosten werden nicht auf die anordnenden Behörden überwälzt. Es kann mit einer Anbieterin einen späteren Beginn der Datenübertragung vereinbaren. Dieser richtet sich nach den technischen Möglichkeiten der Anbieterin und kann spätestens auf den Zeitpunkt der Aufhebung der regionalen Dienststellen festgelegt werden.[15]

5 Die Internet-Anbieterinnen übertragen vom 1. April 2003 an die Daten aus jeder Überwachung dem Dienst. Vorher müssen sie die Auskünfte nach Artikel 14 BÜPF erteilen und vorhandene Verkehrsdaten des E-Mail-Verkehrs übermitteln.

6 ...[16]

Art. 36*a*[17] Übergangsbestimmung zur Änderung vom 23. Juni 2004

Anbieterinnen von Fernmeldediensten müssen von ihren Kundinnen und Kunden, deren Prepaid-SIM-Karte nach dem 1. November 2002 in Betrieb genommen worden ist, bis zum 31. Oktober 2004 die Daten nach Artikel 19*a* erfassen. Nach Ablauf dieser Frist sind die Nummern der nicht registrierten Kundinnen und Kunden ausser Betrieb zu nehmen.

Art. 37 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2002 in Kraft.

Diese Änderung tritt am … 2011 in Kraft.

Begriffe und Abkürzungen

1. Internet-Anbieterin: Fernmeldedienstanbieterin oder der Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien (Netzprotokoll im Internet [Internet Protocol]) unter Verwendung von IP-Adressen anbietet;
2. Betreiberinnen von internen Fernmeldenetzen oder Hauszentralen: die Personen, die über die Beschaffung, die Erstellung und den Betrieb dieser Einrichtungen entscheiden;
3. Echtzeit-Überwachung: das Abfangen in Echtzeit und die simultane, leicht verzögerte oder periodische Übertragung der Post- oder Fernmeldeverkehrsdaten, inklusive der Nutzinformationen, durch die Anbieterinnen von Post- oder Fernmeldediensten gemäss den Angaben der Überwachungsanordnung;
4. rückwirkende Überwachung: die Herausgabe der Verkehrs- und Rechnungsdaten der zurückliegenden sechs Monate durch die Anbieterinnen von Post- oder Fernmeldediensten;
5. Direktschaltung: direkte Übertragung des Fernmeldeverkehrs der überwachten Person vom Dienst an die anordnende Behörde;
6. Nutzinformationen: der Anteil des zu überwachenden

Fernmeldeverkehrs, welcher die zwischen Benutzenden bzw. zwischen deren Endeinrichtungen ausgetauschten Informationen (z.B. Laute, Telefax, E-Mails und Daten) enthält;

7. Verkehrs- und Rechnungsdaten: die Informationen, die von der Anbieterin über den Post- oder Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern aufgezeichnet werden, um die Tatsache der Postsendung oder der Kommunikation und die Rechnungsstellung zu belegen;
8. Adressierungselemente: Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Rufnummern und Kurznummern (Art. 3 Bst. f des Fernmeldegesetzes vom 30. April 1997 9 - FMG);
9. Kommunikationsparameter: die Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind (Art. 3 Bst. g FMG);
10. E.164-Nummer: Adressierungselement des Nummerierungsplans E.164 (vgl. das 2. Kapitel der Verordnung vom 6. Oktober 1997 über die Adressierungselemente im Fernmeldebereich10-AEFV);
11. IMEI-Nummer (IMEI: International Mobile Equipment Identity): internationale Nummer zur Identifizierung von Mobiltelefonie-Geräten;
12. IMSI-Nummer (IMSI: International Mobile Subscribers Identity): internationale Nummer, die zur Identifikation der Teilnehmerin oder des Teilnehmers in einem Mobilfunknetz dient;
13. IP-Adresse (Internet-Protokoll-Adresse): Adresse, die alle verbundenen Geräte in einem Informatiknetzwerk identifiziert, die das Internet-Protokoll benutzen;
14. MAC-Adresse (Media Access Control Address): Hardware-Adresse, die in einer Netzwerkkarte- oder einem Netzwerkadapter hinterlegt ist und als eindeutige Adresse auf der Ebene der Sicherungsschicht gebraucht wird (OSI-Schicht 2);

Technik-asut: Im Zusammenhang mit dem MAC-sublayer kann die Schicht 2 nur als Sicherungsschicht bezeichnet werden, wenn darüber ein Logical Link Control (LLC) Sublayer eingesetzt wir, der zur HDLC Familie gehört und in der Lage ist, Übertragungsfehler zu korrigieren.

IEEE 802.3
1.4.212 MAC frame: Consists of the Destination Address, Source Address, Length/Type field, MAC Client Data, Pad (if required), and Frame Check Sequence.

Generell muss in Frage gestellt werden, ob eine Verordnung der richtige Ort ist, die Technik von Protokollarchitekturen zu erklären.

15. URI (Uniform Resource Identifier): Identifikator einer Ressource im Internet (Webseiten, Dateien, Webservices, SIP-Adresse usw.);
16. SIM-Nummer (SIM: Subscriber Identity Module): Serien-Nummer der SIM Karte, die die Karte eindeutig identifiziert ;
17. Cell ID: unveränderter Zell-Identifikator (Cell Global Identification) der Mobiltelefonie;
18. Umschlaginformationen: Adressierungselemente, die den Datagrammen eines E-Mail angehängt werden;
19. Kopf-Informationen: Informationen, die dem Inhalt einer Meldung vorangestellt sind;
20. Dial-up: Einwahl-Internetzugang über Telefonverbindungen (Analog-Modem oder ISDN);
21. DSL (Digital Subscriber Line): Breitband-Internetzugang mittels Bitübertragungsschicht auf einer Teilnehmeranschlussleitung, der einen hohen Datenfluss erlaubt;
22. xDSL: Gruppe von Techniken, die mit der DSL-Technologie verwandt sind. Der Buchstabe «x» steht für diverse Abkürzungen, mit denen die verschiedenen DSL-Technologien bezeichnet werden;
23. FTTH (Fiber To The Home): Glasfaserleitung bis zur Wohnung des Teilnehmers;
24. Kabelmodem: Modemtyp, der es erlaubt, sich mit dem Internet über ein Ka-belfernsehnetz zu verbinden;
25. SIM-Karte (SIM Subscriber Identity Module): Chipkarte, die zur Identifikation der Teilnehmerin oder des Teilnehmers in einem Mobilfunknetz dient;
26. Prepaid SIM-Karte: SIM-Karte, bei welcher die Kundenbeziehung für Mobiltelefone nicht über ein Abonnementsverhältnis aufgenommen wird;
27. GPRS (General Packet Radio Service): Mobiltelefoniedienst, der die paketvermittelte Datenübertragung über GSM erlaubt;
28. GSM (Global System for Mobile Communications): Standard der zweiten Mobilfunk-Generation;
29. UMTS (Universal Mobile Telecommunications System): Standard der dritten Mobilfunk-Generation;
30. LTE (Long Term Evolution): Standard der vierten Mobilfunk-Generation;
31. OSI-Referenzmodell (Open Systems Interconnection): Modell nach ISO-Norm 7498, welches zur Beschreibung offener

Kommunikationsarchitekturen in Computernetzen dient;
32. OSI-Schicht 2: Sicherungsschicht (engl. Data Link Layer) nach dem OSI-Referenzmodell;
33. OSI-Schicht 3: Vermittlungsschicht (engl. Network Layer) nach dem OSI-Referenzmodell;
34. Ethernet: Familie von Netzwerktechnologien der OSI-Schichten 1 und 2 auf der Basis der IEEE-Norm 802.3;
35. SIP (Session Initiation Protocol): standardisiertes Signalisierungs-Protokoll der IETF für die Steuerung von IP-Telefonie und Multimediakommunikation (Sprache, Audio, Video, Fax usw.);
36. SMTP (Simple Mail Transfer Protocol): Protokoll für die Übermittlung von E-Mail in Computernetzen ;
37. Instant Messaging (sofortige Nachrichtenübermittlung): synchrone Echtzeitkommunikation zwischen zwei oder mehr Teilnehmern. Es gibt eine Vielzahl von Instant Messaging Diensten und es werden zum Teil proprietäre Protokolle verwendet. Neben Textnachrichten können häufig auch Multi-media-Inhalte übertragen werden.
38. VoIP (Voice over IP auch IP-Telefonie oder Internet-Telefonie): Technik, die es erlaubt, über das IP Protokoll zu telefonieren;
39. VPN (Virtual Private Network): ein virtuelles Computernetz mit gekapselter Datenübertragung zwischen 2 oder mehr vernetzten Geräten;
40. Wi-Fi: Standard für kabellose Netzwerke nach der IEEE-Norm 802.11;
41. Wimax (Worldwide Interoperability for Microwave Access): Standard für kabellose Netzwerke nach der IEEE-Norm 802.16;
42. WLL (Wireless Local Loop): drahtloser Teilnehmeranschluss, der eine Alternative zum leitungsgebundenen Anschlussnetz darstellt;
43. IEEE (Institute of Electrical and Electronics Engineers): gemeinnützige Organisation, die die Veröffentlichung der Normen, die von den Mitgliedern der Organisation verfasst werden, sicherstellt;
44. IETF (Internet Engineering Task Force): internationale, informelle Organisation, die die meisten Internetstandards erarbeitet;
45. ISO (International Organization for Standardization): weltweite Organisation für die Erarbeitung und Veröffentlichung internationaler Normen;
46. ITU (International Telecommunication Union): internationale Organisation der Vereinten Nationen, die sich dem Wachstum und der nachhaltigen Entwicklung von Telekommunikations- und Informationstechnologie widmet;
47. ITU-T: Bereich der ITU, der Empfehlungen im Bereich der Telekommunikationsstandardisierung herausgibt.

COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

29 de juillet, 2011

Patrick Schöpf
Centre de services informatiques CSI-DFJP
Service Surveillance de la correspondance
par poste et télécommunication (SCPT)
Fellerstrasse 15, 3003 Berne

Le document a été transmit par email et par fax le 29 juillet 2011

Re: Projet d'Ordonnance sur la Surveillance de la Correspondance par Poste et Télécommunication (OSCPT)

La Computer & Communications Industry Association (CCIA) est en faveur des marchés libres et des systèmes et des réseaux ouverts. Les membres de CCIA, qui participent dans le secteur de l'informatique et de la communication, vont des petits 'start-ups' jusqu'aux plus grands entreprises du secteur. Les membres de CCIA occupent près d'un million des personnes dans le monde et réalisent un chiffre d'affaires de plus de 200 milliards de dollars. CCIA et ses membres soutiennent le principe d'une concurrence économique qui est « libre, juste, et sans limite ».

CCIA, en accord avec les commentaires émis par des autres associations du secteur de la télécommunications et de l'informatique telles que SWICO et ASUT, émets de sérieuses et nombreuses réserves à propos du projet d'Ordonnance sur la Surveillance de la Correspondance par Poste et Télécommunication (OSCPT), qui vise à étendre les

Washington 900 Seventeenth Street NW Suite 1100 Washington, DC 20006, USA Tel: +1 202 783 0070 Fax: +1 202 783 0534
Brussels 11 Rond Point Schuman Suite 417 B-1040 Brussels, Belgium Tel: +32 2 256 7592
Geneva Chemin des Tines 17 1260 Nyon, Switzerland Tel: +41 22 362 02 38 Fax: +41 22 594 85 44

obligations mises à la charge des entreprises en regard de leur coopération dans le cadre de la lutte contre les activités criminelles.

Nous émettons en premier lieu de sérieux doutes quant au processus d'adoption de l'Ordonnance lui-même. Nous sommes d'avis qu'en adoptant un procédé simplifié, le Conseil Fédéral est potentiellement en infraction de la législation Suisse. De plus, le Conseil Fédéral n'a toujours pas publié les conclusions rendues à propos de la révision du texte de la Loi fédérale sur la Surveillance de la Correspondance par Poste et Télécommunication (LSCPT). Enfin, le processus de consultation relatif à l'OSCPT n'a pas été suffisamment étendu.

Nous avons également de sérieux doutes quant au contenu même du projet d'Ordonnance. Toute une série de concepts nouveaux y sont introduits, mais trop peu précisément définis, créant ainsi un flou juridique. Certaines mesures proposées apparaissent en outre clairement disproportionnées et déraisonnables. De plus, le Conseil Fédéral n'a pas suffisamment jaugé les conséquences de l'Ordonnance au-delà des frontières de la Suisse.

En résumé, nous demandons que le Conseil Fédéral abandonne le projet dans son ensemble ou bien en reporte l'examen, après adoption définitive de la LSCPT, afin d'adapter l'OSCPT en conséquence.

Washington 900 Seventeenth Street NW Suite 1100 Washington, DC 20006, USA Tel: +1 202 783 0070 Fax: +1 202 783 0534
Brussels 11 Rond Point Schuman Suite 417 B-1040 Brussels, Belgium Tel: +32 2 256 7592
Geneva Chemin des Tines 17 1260 Nyon, Switzerland Tel: +41 22 362 02 38 Fax: +41 22 594 85 44

Remarques spécifiques à propos de la réponse au processus consultatif relatif à l'Ordonnance sur la Surveillance de la Correspondance par Poste et Télécommunication (OSCPT), au 29 Juillet 2011.

1. Nous émettons de sérieux doutes quant au processus d'adoption

a. Un processus consultatif insuffisant

CCIA regrette que seuls quelques interlocuteurs aient été invités à commenter le projet d'Ordonnance. Le système politique suisse extrêmement sophistiqué, s'appuyant notamment sur des mécanismes de démocratie directe, invite tout le monde à contribuer et à partager divers points de vue et avis sur quelque question que ce soit, dans le cadre de l'adoption d'un nouveau texte de loi. Les modifications ou extensions du régime actuel du Service Surveillance de la correspondance par poste et télécommunications soulèvent des problématiques extrêmement délicates et complexes, emportant des effets tant sur les entreprises que sur les citoyens. Le Département Fédéral de la Justice et de la Police (DFJP) essaie aujourd'hui de procéder à ces modifications sans se soumettre à la procédure de consultation et en ignorant les procédures législatives en procédant à une simple audition de quelques interlocuteurs choisis. Ceci constitue une pratique peu commune, et marque une attitude dénégatoire du respect et du sens des responsabilités légitimement attendus d'une autorité fédérale en pareille circonstance, *a fortiori* concernant une modification législative comportant autant d'aspects sensibles.

b. LSCPT et OSCPT

Il apparaît évident que la révision en cours de la Loi fédérale sur la Surveillance de la Correspondance par Poste et Télécommunication devrait être achevée avant l'examen d'une nouvelle OSCPT. La révision des Ordonnances relatives à la LSCPT devrait en effet se baser sur le texte définitif et adopté de la LSCPT, et non sur la version actuelle de la loi. Ni le

parlement ni les acteurs du marché concerné n'ont été tenu informés des résultats de la procédure de consultation menée à propos de la LSCPT qui s'est achevé en 2010. Dans ce contexte d'incertitude juridique, il est d'autant plus difficile de comprendre comment une nouvelle OSCPT pourrait être légitimement entérinée.

c. **Questions Constitutionnelles**

Nous sommes d'avis que la modification de l'Ordonnance ne peut être menée par le Conseil Fédéral que dans les limites des pouvoirs qui lui sont conférés par la section 164 de la Constitution Suisse. Cette section réserve au Parlement seul le droit d'adopter des provisions créant, ou altérant de manière substantielle, un régime juridique, par le biais d'une Loi Fédérale. Nous pensons que les propositions de modifications de l'Ordonnance faites à ce jour, étendent son champ d'application de telle manière qu'elles rendent *de facto* le Conseil Fédéral incompétent et imposent un examen du texte par la voie parlementaire. Nous pensons en conséquence que la procédure d'adoption suivie actuellement est potentiellement anticonstitutionnelle, *a fortiori* compte tenu de la révision actuelle de la Loi à laquelle l'Ordonnance se rattache.

2. Nous émettons des réserves quant au fond du projet d'Ordonnance

a. **Concept de "Fournisseurs Internet"**

Le texte actuel de l'OSCPT s'applique aux '*fournisseurs d'accès à Internet*'. A titre comparatif, la section 1 al. 2 let. e du projet de l'OSCPT fait référence aux '*fournisseurs de services de télécommunication, y compris aux* ***fournisseurs Internet***'. Une modification similaire est proposée à l'Art. 8, al. 1 du projet de l'OSCPT[1], étendant de fait la notion de fournisseurs de services Internet, au-delà des fournisseurs d'accès à Internet. Ceci constitue une tentative visant à multiplier le nombre d'interlocuteurs pouvant être appelés à coopérer avec les autorités. Si nous comprenons la nécessité de telles mesures de

[1] Relatif à la création et l'exploitation d'un centre de traitement des données recueillies lors de la surveillance

surveillance dans le cadre de la prévention et de la punition des activités criminelles, la définition de *'fournisseurs Internet'* est si vague[2] qu'elle crée une insécurité juridique importante pour les entreprises opérants en Suisse et, potentiellement, des conflits de lois aux conséquences graves pour les entreprises opérant hors de Suisse, mais pouvant se trouver sujet à l'application de l'OSCPT. Ceci pourrait conduire les autorités à disposer d'un très large éventail d'interlocuteurs dans divers domaines d'activités, proposant des services qui bien qu'utilisant tous dans une certaine mesure des protocoles IP, sont profondément différents tant sur le plan technologique que de leurs infrastructures. Par conséquent, un large panel d'entreprises offrant des services incluant, sans pour autant se limiter, à des service VoIP, de messagerie instantanée, de réseaux sociaux, de forums Internet, WLAN, ou tout autre service ou infrastructure basés sur un protocole IP, pourrait être contraints de mobiliser d'importantes ressources humaines et financières afin de se mettre en conformité avec la loi. De telles obligations pouvant éventuellement interférer avec la liberté économique (comprenant notamment le libre accès à une activité économique lucrative privée et son libre exercice), garantie par la constitution, une base légale précise devient une absolue nécessité[3]. Connaissant la nature sensible et onéreuse des obligations en question, une définition des services et entreprises concernées devrait être établic et limitée à ceux dont la coopération se justifie par les besoin impérieux de l'application de la loi. Celle-ci devrait s'accompagner d'une liste des exigences techniques requises et décrire comment les mesures de surveillance seront implantées à la lumière des différences existantes entre les fournisseurs de services utilisant les protocoles IP connus à ce jour. Les entreprises établies en Suisse et fournissant des services relatifs à l'Internet, sans pour autant fournir de

[2] Un fournisseur Internet est définie comme un « *fournisseur de services de télécommunication ou le secteur d'un fournisseur de services de télécommunication qui offre une prestation publique de transmission d'informations sur la base de la technologie IP (protocole du réseau internet (Internet Protocol)) et d'adresses IP* »

[3] Comme récemment indiqué dans la décision du Tribunal Administratif Fédéral N° A-8284/2010, rendue le 21 Juin 2011

services de télécommunications ou de réseaux sociaux, devraient expressément être exclus de la définition de 'fournisseurs Internet'.

b. **L'impact au-delà de la Suisse**

i. **Compétence juridictionnelle**

Nous croyons impératif que le Conseil Fédéral clarifie son approche quant à la compétence juridictionnelle des cours Suisses en matière d'Internet (et notamment vis-à-vis des services fournis depuis l'étranger mais accessibles depuis la Suisse), et ce faisant, garde à l'esprit le principe de territorialité de la loi Suisse, ainsi que l'exemple que sa décision pourrait constituer pour des pays ayant des mécanismes constitutionnels et juridiques de protection de leurs citoyens moins développés que ceux de la Suisse.

ii. **"Mesures de surveillance en rapport avec l'étranger"**

La Section 24c traite des 'mesures de surveillance en rapport avec l'étranger'. Nous sommes convaincus que le Conseil Fédéral est conscient de l'impact négatif que l'extension des mesures de surveillance, à des individus vivant dans d'autres pays et jouissant de la protection des lois nationales de ces derniers, pourrait causer. Cette section nécessite par conséquent une précision quant aux services, opérateurs, et données qui en feraient l'objet. Une telle précision se devra d'être détaillée et exhaustive afin d'éviter toute ambiguïté ou incertitude juridique.

c. **Proportionnalité des mesures**

i. **Mots de Passe**

CCIA est d'avis qu'il est déraisonnable d'imposer la révélation des mots de passe des utilisateurs aux autorités.

ii. **Concept de "surveillance rétroactive"**

La Section 24 du projet d'Ordonnance fait référence à deux types de surveillance, en *'temps réel'* ou *'rétroactif'*. Le concept de surveillance rétroactive devra être clarifié afin d'éviter la création d'obligations

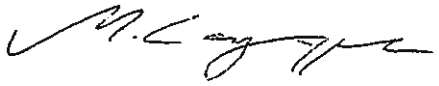
Washington 900 Seventeenth Street NW Suite 1100 Washington, DC 20006, USA Tel: +1 202 783 0070 Fax: +1 202 783 0534
Brussels 11 Rond Point Schuman Suite 417 B-1040 Brussels, Belgium Tel: +32 2 256 7592
Geneva Chemin des Tines 17 1260 Nyon, Switzerland Tel: +41 22 362 02 38 Fax: +41 22 594 85 44

disproportionnées. Toute problématique relative à la rétention de données qui serait requise pour se conformer au principe de surveillance rétroactive devra être clairement discutée et établie en accord avec les acteurs du marché. La rétention et l'obligation de révélation des données imposent aux fournisseurs d'avoir des politiques, des systèmes et des outils adaptés, nécessitant la mobilisation de ressources financières et humaines, en conséquence de quoi, des délais réalistes devront être agréés pour permettre la mise en œuvre de ces nouvelles obligations

iii. **La possibilité d'extension discrétionnaire des mesures**

L'Art. 25, paragraphe 5 du projet d'Ordonnance dispose que les mesures de surveillance listées dans l'OSCPT, et en particulier les dispositions aux articles 24a et 24b, traitant des communications Internet, ne sauraient être considérées comme exhaustives et que, sur demande des autorités en charge de l'application de la loi, les fournisseurs Internet pourraient être amené à procéder à d'autres mesures de surveillance non expressément prévues dans l'Ordonnance. Cette section crée un flou juridique et permet aux autorités de changer ou d'étendre les mesures de surveillance hors de tout examen parlementaire. Cette pratique n'est pas appropriée étant donné la nature délicate du sujet et la portée des éventuelles obligations mises à la charge des fournisseurs de services.

Matthias Langenegger



Représentant Adjoint à Genève
Computer & Communications
Industry Association (CCIA)

Washington 900 Seventeenth Street NW Suite 1100 Washington, DC 20006, USA Tel: +1 202 783 0070 Fax: +1 202 783 0534
Brussels 11 Rond Point Schuman Suite 417 B-1040 Brussels, Belgium Tel: +32 2 256 7592
Geneva Chemin des Tines 17 1260 Nyon, Switzerland Tel: +41 22 362 02 38 Fax: +41 22 594 85 44

CENTRE PATRONAL

Route du Lac 2
1094 Paudex

Case postale 1215
1001 Lausanne

Tél. 021 796 33 00
Fax 021 796 33 11
info@centrepatronal.ch
www.centrepatronal.ch

CCP 10-13744-9
TVA/MWSt 270 039

Monbijoustrasse 14
Postfach 5236
3001 Bern
Tel. 0313 909 909
Fax 0313 909 903
cpbern@centrepatronal.ch

CONFEDERATION SUISSE
Département fédéral de justice et police
Centre de services informatiques
CSI-DFJP
Service Surveillance de la correspondance par poste et télécommunication
Unité droit et contrôle de gestion
A l'intention de M. Patrick Schöpf
3003 BERNE

Paudex, le 19 juillet 2011
SB/ra

Modification de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT) ainsi que de l'ordonnance sur les émoluments et les indemnités en la même matière (OEI-SCPT)

Réponse à la consultation

Monsieur,

Nous avons pris connaissance du projet cité en référence et, comme nous le faisons habituellement lors d'une procédure de consultation, nous prenons la liberté de vous communiquer ci-après notre position.

I. Bases légales et évaluation du besoin actuel de réformer l'OSCPT

L'art. 92 al. 1 de la Constitution fédérale (Cst.) accorde à la Confédération la compétence de régir le domaine des services postaux et des télécommunications. La Confédération est aussi compétente pour légiférer en matière de droit pénal et de procédure pénale alors que l'organisation et l'administration de la justice pénales restent en principe du ressort des cantons (art. 123 Cst.). Sur cette base constitutionnelle, une loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) règle les modalités de la surveillance qui peut être ordonnée dans le cadre d'une procédure pénale fédérale ou cantonale, lors de l'exécution d'une demande d'entraide pénale internationale ou dans le contexte de la recherche et du sauvetage de personnes disparues (art. 1 al. 1 LSCPT).

Le Département fédéral de justice et police (DFJP) prépare actuellement une révision de la LSCPT afin de l'adapter à l'évolution technique, notamment face au développement d'internet et de la téléphonie sur internet qui peuvent offrir de nouveaux moyens pour faciliter la commission d'infractions pénales. Dans le cadre de cette réforme, le DFJP a envoyé en consultation un projet de loi durant le printemps 2010 (le Centre Patronal y a répondu favorablement sous réserve d'un

certain nombre de remarques liées surtout à la sauvegarde des droits fondamentaux; voir la réponse à la consultation du 10.8.2010 : http://www.centrepatronal.ch/index.php?id=1051).

Dans la lettre d'accompagnement du DFJP aux présents projets de modification d'ordonnances, il est fait mention qu'avec la révision de la LSCPT, tant les processus liés aux activités de surveillance que les émoluments et indemnités y afférents seront à nouveau revus. Se pose dès lors la question de savoir s'il est indispensable de soumettre maintenant l'OSCPT et l'OEI-SCPT à une réforme partielle.

Le rapport explicatif du projet de réforme OSCPT/OEI-SCPT répond à cela par le constat que la technologie analogique de communication (téléphonie, télécopie etc.) est sur le point de disparaître au profit de la technologie internet et que, face à cette situation, les autorités de poursuite pénale se plaignent que les prescriptions de l'OSCPT ne sont plus à jour et qu'une poursuite pénale efficace est de ce fait rendue très difficile (rapport, p. 1). En outre, les autorités de poursuite et les juridictions pénales estiment que la liste des mesures de surveillance prévue dans l'OSCPT actuelle n'est pas exhaustive, ce qui a pour conséquence que le service fédéral chargé de la surveillance de la correspondance par poste et télécommunication (service SCPT), ainsi que les fournisseurs de ces services doivent parfois exécuter des mesures qui ne figurent pas explicitement dans l'OSCPT. En effet, les décisions que le service SCPT est appelé à rendre à l'intention de fournisseurs de services de télécommunication peuvent faire l'objet de recours judiciaires. Ainsi, le Tribunal fédéral a été amené à soutenir à plusieurs reprises, en référence à la LSCPT, des pratiques plus étendue de la surveillance que ne le prévoit l'OSCPT (rapport, p. 2).

Cette situation est génératrice d'insécurité juridique dans un domaine qui touche de près les droits fondamentaux des individus. De plus, l'exécution de mesures de surveillance non prévues par l'OSCPT occasionne des coûts pour le service SCPT et pour les fournisseurs de services de télécommunication qui risquent de ne pas être indemnisés.

Nous sommes de l'avis que dans un domaine aussi sensible que la surveillance par des autorités publiques de communications privées, il est indispensable qu'un dispositif légal complet et à jour délimite et justifie précisément dans quelle mesure l'intérêt public doit primer sur la protection de la vie privée d'une part, et que soit défini clairement comment se répartissent, en toute circonstance, les coûts occasionnés par cette surveillance, d'autre part. Il existe donc des raisons valables, qui dépassent l'unique prise en compte de l'évolution rapide de la technologie, pour réviser l'OSCPT – et l'OEI-SCPT y corrélée – sans attendre l'achèvement de la réforme de la LSCPT.

II. Appréciation de la réforme de l'OSCPT quant au fond

Un bon nombre d'adaptations de l'OSCPT sont de nature purement linguistique. La plupart clarifie le texte à la lumière de l'expérience pratique. Mais, certaines de ces modifications linguistiques ont en plus des implications juridiques.

Il en va de la sorte pour l'art. 1 al. 2 let. e OSCPT où la notion de « fournisseurs d'accès à internet » est remplacé par « fournisseur internet » (un changement qui se répète dans d'autres dispositions). Ce nouveau terme plus ouvert étend le champ d'application personnel de l'OSCPT et accroît donc le nombre d'acteurs économiques touchés potentiellement par une mesure de surveillance. Certes,

l'évolution technologique et la réalité socio-économique font que certains fournisseurs offrent des prestations de services internet sans proposer eux-mêmes l'accès au réseau au sens étroit. D'un autre côté, il existe un intérêt public prépondérant, tel que la lutte contre la cybercriminalité, pour que la télécommunication par internet puisse, dans le cadre strict de la légalité, être surveillée. La logique économique réclame également que tous les fournisseurs de services internet en Suisse se voient appliquer les mêmes règles (*level playing field*), y compris sous l'angle d'une possible soumission à une mesure de surveillance.

Certaines normes de l'OSCPT doivent être modifiées du fait de l'entrée en vigueur au 1er janvier 2011 du Code de procédure pénale fédéral qui a entraîné l'abrogation de divers articles de la LSCPT, ce qui induit, par ricochet, des adaptations de l'OSCPT (p. ex. art. 11 al. 1 let. d, art. 15 al. 1 let. d et i, art. 23 let. d, art. 25 al 2). Vu que la sécurité du droit dépend de la cohérence de l'ordre normatif, il n'y a rien à y objecter.

D'autres dispositions de l'OSCPT doivent, pour rester pertinentes, tenir compte de l'évolution technologique (p. ex. art. 16 et 23 let. g). A cet égard, nous observons en particulier qu'en matière de téléphonie mobile, la recherche par champ d'antennes permet désormais de retrouver rétroactivement les communications effectuées à un endroit et durant un laps de temps déterminés. Couplée à l'identification des numéros appelant et appelés, cette méthode limite la saisie à une ou plusieurs conversations précises, ce qui rend l'écoute/surveillance très ciblée et donc plus proportionnée et plus respectueuse des droits individuels (voir art. 16 let. e OSCPT). Concernant la surveillance d'internet, nous remarquons la refonte complète de l'art. 24 OSCPT, d'une part pour rattraper l'état actuel de la technologie et, d'autre part, pour intégrer la pratique autorisée par la jurisprudence. On ne peut que saluer le fait que les autorités de poursuite pénale bénéficieront en matière de lutte contre la cybercriminalité à nouveau d'un cadre réglementaire qui soit juridiquement précis et adapté aux possibilités techniques. De surcroît, il est heureux de voir sous l'angle du respect du principe de la proportionnalité, ainsi que de celui des droits fondamentaux que la réforme de l'art. 24 OSCPT a été complétée par l'introduction de deux articles 24a et 24b qui définissent en détail quels types de surveillance d'internet sont autorisés en temps réel et rétroactivement. Toujours au regard du renforcement de la légalité et de la sécurité juridique dans ce domaine délicat car constitutif d'une intrusion dans la vie privée, il faut signaler le nouvel art. 16a qui détermine les possibilités de surveillance de la téléphonie mobile en cas de recherche et sauvetage de personnes disparues, ainsi que l'art. 16b, respectivement 24c, qui énoncent les mesures pouvant être prises sur les réseaux de téléphonie mobile et d'internet en lien avec l'étranger.

Enfin, les articles 25 (*Mise en œuvre de la surveillance*), 26 (*Obligations des fournisseurs Internet*) et 27 (*Renseignements sur les usagers d'Internet*) OSCPT ont également été retravaillés. Les articles 25 et 27 portent un soin particulier à redéfinir l'information qui doit être transmise au service SCPT par les fournisseurs internet (l'art. 25 al. 4 définit la correspondance électronique d'une personne sous surveillance selon les standards européens ETSI et l'art. 27 al. 1 et 2 énonce les données d'identification informatique et personnelle à fournir); l'art. 26 précise quant à lui jusqu'à quel point le fournisseur internet doit pouvoir surveiller le trafic électronique qui transite par son infrastructure.

Ces précisions sont évidemment les bienvenues au regard de la sécurité juridique, de la proportionnalité des mesures prises et de la protection des droits individuels, et elles visent bien sûr à rendre à nouveau efficaces les mesures de sur-

veillance. Toutefois, l'extension des articles 25 à 27 OSCPT – ainsi que l'ensemble de la réforme proposée – induira des coûts. Par conséquent, il faut aussi examiner les modifications apportées à l'ordonnance sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication (OEI-SCPT) qui découlent de la réforme de l'OSCPT.

III. Appréciation de la réforme de l'OEI-SCPT

Malgré les changements apportés à l'OSCPT concernant les mesures de surveillance en matière de téléphonie mobile, l'adaptation de l'OEI-SCPT ne touche pas aux émoluments et indemnités prévus dans ce domaine (voir art. 2 A. OEI-SCPT). La recherche par champ d'antennes, la recherche et le sauvetage de personnes disparues et les mesures de surveillance liées à l'étranger donneront droit à des émoluments, à payer par les autorités de poursuite pénale, et à des indemnités à verser aux fournisseurs de service de télécommunication; mais il s'agit là que de la formalisation d'une pratique déjà observée actuellement par le service SCPT (voir rapport explicatif, p. 16).

Concernant la surveillance d'internet, il faut se souvenir que la réforme de l'OSCPT a pour but de réglementer celle-ci bien plus largement qu'auparavant. De ce fait, le projet de réforme revoit complètement l'art. 2 B. OEI-SCPT qui régit le système d'émoluments et d'indemnités à payer lors de la mise en œuvre de mesures de surveillance du trafic internet. Selon le DFJP, la révision de l'OSCPT et de l'OEI-SCPT n'aura à court terme pas de conséquence financière ou en matière de personnel pour la Confédération. A moyen terme, le Département pense même que le service SCPT pourra se servir de processus standardisés de surveillance et que cela entraînera une baisse des dépenses. D'un autre côté, les autorités de poursuite pénale devront faire face aux frais liés aux nouvelles possibilités d'investigation. Mais le DFJP estime qu'à ce niveau les coûts seront raisonnables et proportionnés au regard du gain d'efficacité issu des nouveaux moyens de surveillance et d'investigation (rapport, p. 20-21).

En revanche, il subsiste la question des frais d'investissement qu'auront à consentir les fournisseurs de service de télécommunication (FST) pour garantir l'exécution de mesures de surveillance sur internet, qui pourront à l'avenir être nettement plus variées. Le rapport du DFJP reste très lapidaire à ce sujet (voir p. 20) et pour cause, puisqu'il s'agit de frais supportés par des privés et donc de coûts qui, aux yeux de l'administration fédérale, sont externes.

Nous ne pouvons évaluer si les indemnités nouvellement prévues par l'OEI-SCPT pour des services de surveillance d'internet (art. 2. B) couvriront l'ensemble des frais à prendre en charge par les FST. Nous ignorons aussi si chaque PME active dans le domaine de l'internet sera en mesure de se doter des ressources nécessaires pour pouvoir exécuter les mesures de surveillance qui pourraient lui être imposées. Certes, le service SCPT est censé collaborer étroitement avec les FST concernés et il doit même les aider à trouver la solution technique (achat/location d'appareils et d'interfaces pour la surveillance d'internet qui leur est adaptée; voir www.ejpd.admin.ch la rubrique SCPT). Cependant, il serait inadmissible de déléguer à des acteurs privés des tâches qui sont d'intérêt public sans les indemniser à la hauteur des frais qu'ils subissent (y compris les investissements à consentir; voir à ce propos déjà les conclusions de notre réponse du 10.8.2010 à la consultation sur la réforme de la LSCPT, précité). Cas échéant, le montant des indemnités devra être revu sur la base de l'expérience.

Vu la révision de la LSCPT en cours qui engendrera de nouvelles modifications de l'OSCPT et de l'OEI-SCPT, les milieux de l'économie du net auront, en cas de besoin, à nouveau l'occasion de pouvoir s'exprimer sur l'important enjeu d'une répartition équitable des coûts occasionnés par la nécessité – par ailleurs non contestée – de pouvoir ordonner la surveillance de la téléphonie mobile et des services internet en cas de risque d'infraction pénale ou de recherche de personnes disparues.

❖ ❖ ❖

Pour les raisons exposées, mais moyennant la prise en compte d'un règlement équitable entre acteurs publics et privés des frais induits, nous pouvons approuver les réformes partielles de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT), ainsi que de l'ordonnance sur les émoluments et les indemnités en la même matière (OEI-SCPT).

❖ ❖ ❖

En vous remerciant de l'attention que vous voudrez bien porter à la présente, nous vous prions d'agréer, Monsieur, l'expression de nos sentiments les meilleurs.

CENTRE PATRONAL

Stéphane Bloetzer

Chaos Computer Club Zürich
Luegislandstrasse 485
8051 Zürich

Informatik Service Center – ISC EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Bereich Recht und Controlling
z.Hd. Patrik Schöpf <patrik.schoepf@isc-ejpd.admin.ch>
3003 Bern

VÜPF – Anhörung zu den vorgeschlagenen Änderungen: Stellungnahme des Chaos Computer Clubs Zürich (CCCZH)

Zürich, den 15. Juli 2011

Sehr geehrte Damen,
sehr geehrte Herren.

Der Chaos Computer Club Zürich, kurz CCCZH[1], möchte hiermit Stellung zu den geplanten Änderungen der „*Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*“ (VÜPF) beziehen.

Dem Namen nach soll die VÜPF die Überwachung des *persönlichen* Nachrichtenverkehrs einer verdächtigen Person nach genehmigter Anordnung durch zuständige Stellen regeln. Dabei wird gewollt der Eindruck vermittelt, dass es hierbei nur um die *direkte und persönliche Kommunikation einer Person* geht, die einer Straftat verdächtigt und deren Kommunikation deshalb auf Anordnung hin kontrolliert, archiviert und ausgewertet werden darf.

Auch wenn die zur Zeit gültige Fassung der VÜPF dieser Interpretation durch die sogenannte rückwirkende Überwachung mit der Vorgabe einer verdachts-unabhängigen und langfristigen Speicherung von Kommunikationsdaten in Bezug auf Email-Austausch und (Mobil-)Telefonie schon erheblich zuwiderläuft, öffnen die vorgeschlagenen Änderungen durch ihre unklare und unbestimmte Formulierung – vor allem im *Abschnitt 6: Überwachung des Internets* – einer Protokollierung sämtlicher Internetnutzungen aller Anwender in der Schweiz Tür und Tor. Dem Vorsatz, zu einer transparenteren Überwachungs-Praxis beizutragen und mehr Rechtssicherheit auch für involvierte Firmen wie Internet-Service-Provider (ISP) zu bieten, tragen die vorgeschlagenen Änderungen aus unserer Sicht in keiner Weise Rechnung.

1 Siehe auch: http://ccczh.ch

Für den Chaos Computer Clubs Zürich (CCCZH), der sich den Idealen der informationellen Selbstbestimmung verpflichtet fühlt, ist diese Entwicklung deshalb bedenklich und konsequent abzulehnen.

In den nachfolgenden Abschnitten werden die einzelnen Kritikpunkte an den vorgeschlagenen Änderungen der VÜPF näher ausgeführt. Basierend auf der Kern-Kompetenz des CCCZH, die technischen und politischen Entwicklungen in der digitalen Welt zu begleiten, liegt der Schwerpunkt der Kritik in den Regelungen zum *Abschnitt 6: Überwachung des Internets*. Kritische Anmerkungen zu anderen Abschnitten der Verordnung sind in einem eigenen Kapitel zusammen gefasst.

Abschnitt 6: Überwachung des Internets

Art. 23 Überwachungsanordnung

Internet-Anbieterin

In ***Art. 23 Bst. f*** wird in der Überwachungsanordnung auf die involvierte *Internet-Anbieterin* verwiesen, die in die Überwachung eingebunden und für die Übermittlung der Informationen an die überwachende Stelle zuständig ist. Nach Glossar ist unter einer *Internet-Anbieterin* im Sinne des VÜPF eine Firma zu verstehen, die *kommunikations-basierte IP-Dienstleistungen im Sinne des Fernmeldeverkehrs (fernmeldetechnische Übertragungen)* wie zum Beispiel VoIP (Internet-Telefonie) oder Email anbietet und deshalb unter die Regelungen und Anordnungen der VÜPF fällt, ohne selbst Internet-Zugangsanbieterin sein zu müssen.

Diese Definition geht von der Annahme aus, dass für einen Dienst (z.B. VoIP) auch nur eine Internet-Anbieterin *zuständig* ist, über die der Dienst abgewickelt wird und die daher auch in der Lage ist, die geforderten Informationen an die überwachende Stelle zu übermitteln.

Auf Grund der technischen Abläufe zum Beispiel bei einer VoIP-Kommunikation (SIP für den Verzeichnisdienst und RTP für die Nutzdatenübertragung) ist dies aber in der Regel nicht der Fall: Die VoIP-Anbieterin verwaltet nur die Benutzerkonten und stellt einen Verzeichnisdienst (ähnlich einem Telefonbuch) zur Verfügung; ob ein VoIP-Gespräch nach einem Lookup (Nachschlagen im Verzeichnis) auch wirklich stattfindet, wann es beginnt und wie lange es dauert oder gar welchen Inhalt das Gespräch hat, kann die VoIP-Anbieterin technisch nicht bestimmen und daher auch nicht übermitteln, da die Daten mittels RTP *an ihr vorbei* übertragen werden (ähnlich dem Datentransport in einen P2P-Netzwerk wie z.B. Torrent).

Eine Überwachung von VoIP-Gesprächen erfordert daher sowohl die koordinierte Überwachung zwischen der VoIP-Anbieterin (SIP) und dem Internet-Zugangsanbieter (RTP) (im Falle einer Echtzeitüberwachung) als auch weitergehenden technischen Aufwand (D/SPI, *Deep/Stateful Packet Inspection*) bei einer Überwachung/Protokollierung/Archivierung des gesamten Internet-Verkehrs aller Nutzer beim Internet-Zugangsanbieter (rückwirkende Überwachung). Die sich daraus

ergebende Totalüberwachung beim Internet-Zugang ist aus Sicht des CCCZH konsequent abzulehnen, da sie Privatsphäre und informationelle Selbstbestimmung verletzt.

Ähnliche Massnahmen einer Totalüberwachung wären auch notwendig, wenn zu überwachende Personen VoIP- und/oder Email-Dienste bei ausländischen Anbietern nutzen. Da sich die erwünschten Überwachungsdaten auch in diesem Fall nur durch aufwendige Analyse des gesamten Internetverkehrs am Internet-Zugang ermitteln lassen, ist auch dies aus Sicht des CCCZH konsequent abzulehnen.

Adressierungselemente

In ***Art. 23 Bst. g*** wird festgelegt, das die Überwachungsanordnung bestimmte technische Adressierungselemente wie zum Beispiel MAC-Adressen, IMSI- und IMEI-Nummern enthalten sollte. Im Glossar der Verordnung wird in Bezug auf diese Adressierungselemente der Eindruck erweckt, als wären diese Elemente unveränderbare und damit identifizierende Merkmale der verwendeten Kommunikations-Endgeräte wie Computer und Handy und somit ihrer Benutzer.

Tatsächlich lassen sich diese Werte aber mit vorhandenem technischen Know-How und vertretbaren Aufwand auf der heute gängigen Hardware verändern.[2] [3] [4] Damit ist die Gefahr gegeben, dass verdächtige Kriminelle diese Adressierungselemente absichtlich verändern, um ihre Kommunikation verschleiern und damit gewollt oder ungewollt *unbeteiligte und unschuldige Dritte* in den Verdacht einer Straftat bringen und zum Ziel einer Überwachung werden lassen, da ISPs nach diesen Angaben Kommunikations- und Inhaltsdaten filtern, sammeln und an die überwachende Behörde weiterleiten.

Fall-Szenario: MAC-Adressen sind z.B. im Falle einer WiFi-Verbindung mit einem offenen WLAN-Hotspot (z.B. einem *Access Point* (AP) in einem Hotel) das einzig zu Verfügung stehende Adressierungselement, um eine Endgerät und damit einen Nutzer zu identifizieren. Wird in einem solchen Fall das Netz zur Begehung von Straftaten verwendet (z.B. Kinderpornographie), kann aus der IP-Adresse des AP-Betreibers und dessen Logdateien bestenfalls die MAC-Adresse des Endgeräts ermittelt werden. Wird daraufhin durch eine Überwachungsanordnung der gesamte zukünftige WiFi-Verkehr überwacht, der von dieser MAC-Adresse aus geführt wird, können dabei wie oben beschrieben die Persönlichkeitsrechte unschuldiger Dritter verletzt werden. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Art. 24 Überwachbare Internetzugänge und Anwendungen

Überwachbare Internet-Zugänge

In ***Art. 24 Abs. 1 Bst. f*** werden explizit Zugänge über OSI Schicht 3 erwähnt. Dies ist

---

2 **MAC-Addresse ändern**: siehe z.B. http://www.mydigitallife.info/how-to-change-or-spoof-mac-address-in-windows-xp-vista-server-20032008-mac-os-x-unix-and-linux/

3 **IMEI ändern auf iPhone4**: siehe z.B. http://www.iclarified.com/entry/comments.php?enid=657

4 **IMSI ändern auf SIM-Karte**: siehe z.B. http://www.nowsms.com/discus/messages/1/42197.html

technisch redundant, da unter ***Art. 24 Abs. 1 Bst. e*** bereits Zugänge nach OSI Schicht 2 erwähnt sind und OSI Schicht 3 notwendigerweise OSI Schicht 2 voraussetzt.

Das explizite Aufführen von OSI Schicht 3 wäre nur verständlich, wenn damit auch Internet-Verkehr, dessen *physikalischer Zugang nicht in der Schweiz stattfindet*, ebenfalls unter die Regelungen des VÜPF fallen soll. Dies würde aber bedeuten, dass auch Angehörige fremder Staaten von den Massnahmen der Vorratsdatenspeicherung (rückwirkende Überwachung) betroffen sein können und dass die Schweiz damit das Territorialitätsprinzip verletzt. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Überwachbare Internet-Anwendungen

In ***Art. 24 Abs. 2 Bst. b*** wird aufgeführt, dass zu den überwachbaren Anwendungen im Internet sogenannte Multimedia-Dienste gehören.

Entgegen den Erklärungen des erläuternden Berichtes[5] zu den geplanten Änderungen an der VÜPF, der unter dieser Kategorie nur explizit Internettelefonie-Systeme wie Skype aufführt, besagt das allgemeine Verständnis von Multimedia aber etwas viel umfassenderes[6]: „Der Begriff Multimedia bezeichnet Inhalte und Werke, die aus mehreren, meist digitalen Medien bestehen: Text, Fotografie, Grafik, Animation, Audio und Video."

Nach dieser Definition ist *jede Webseite im Internet oder jeder andere über das Internet angebotene Dienst* ein Multimedia-Dienst und der Zugriff auf diese Inhalte kann nach VÜPF auch überwacht werden. Da hier rückwirkende Überwachung nicht explizit ausgenommen ist, kann jeder ISP dazu verpflichtet werden, *alle besuchten URLs aller seiner Internet-Kunden zu protokollieren*, zu archivieren und auf Verlangen an die überwachenden Behörden auszuhändigen.

Art. 24a Überwachungstypen (Echtzeit)

Totalüberwachung

In ***Art. 24a Bst. a*** wird die vollständige Weitergabe aller Daten, die über einen überwachten Anschluss übermittelt werden, zu einem erlaubten Überwachungstyp erklärt.

Diese Totalüberwachung steht in direktem Widerspruch zu den Ausführungen in ***Art. 24 Abs. 2 Bst. b***, der die überwachbaren Anwendungen definiert, einschränkt und keine Ausnahmen festlegt. Es liegt nur dann kein Widerspruch vor, wenn unsere Einwände gegen die unklare Formulierung „Multimedia-Dienst" als generischer Internet-Traffic hier genauso verstanden werden.

Adressierungselemente

In ***Art. 24b Bst. b Zif. 5*** wird ebenfalls auf die Protokollierung und Weitergabe von Adressierungselementen wie MAC-Adresse, IMSI- oder IMEI-Nummer verwiesen.

---

5 http://www.bfm.admin.ch/content/dam/data/pressemitteilung/2011/2011-06-08/110608_ber-de.pdf

6 Zitiert nach Wikipedia: http://de.wikipedia.org/wiki/Multimedia

Die zum ***Art. 23 Bst. g*** vorgetragenen Einwände (leichte Manipulierbarkeit dieser Informationen und damit einhergehende Kompromittierung unschuldiger Dritter) sind hier ebenfalls gültig.

Inhalt der Kommunikation

In ***Art. 24a Bst. c*** wird die Überwachung und Weitergabe des Inhaltes in Bezug auf eine überwachte Anwendung nach ***Art. 24 Abs. 2*** festgeschrieben.

Durch die unklare Definition des Begriffes „Multimedia-Dienst“ in ***Art. 24 Abs. 2 Bst. b*** kann dies dazu führen, dass der Inhalt der gesamten Internet-Nutzung überwacht werden kann und dann eine identische Situation wie ***Art. 24a Bst. a*** (Totalüberwachung) bedeutet. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Art. 24b Überwachungstypen (rückwirkend)

Rückwirkende Überwachung basiert auf der verdachtsunabhängigen Speicherung der Kommunikationsdaten aller Internet-Nutzer durch die Internet-Service-Provider (ISPs). Die Verordnung verpflichtet ISPs, die Kommunikationsdaten aller Kunden *ohne genehmigte Anordnung oder eines begründeten Straftatverdachtes* über einen Zeitraum von mindestens sechs Monaten zu archivieren und auf Verlangen den zuständigen Behörden auszuhändigen.

An dieser Stelle kann nur die schon in Bezug auf ***Art. 24 Abs. 2 Bst. b*** geäusserte Kritik wiederholt werden: durch die unklare Formulierung des Begriffes „Multimedia-Dienst“ kann nach geplanter VÜPF jeder ISP dazu verpflichtet werden, *alle besuchten URLs aller seiner Internet-Kunden zu protokollieren*, zu archivieren und auf Verlangen an die überwachenden Behörden auszuhändigen. Diese Form der Vorratsdatenspeicherung halten wir mit den Grundsätzen der informationellen Selbstbestimmung für unvereinbar.

Zudem sind die ISPs für die Vertraulichkeit der gespeicherten Daten verantwortlich. Zahllose Fälle von Datendiebstahl durch interne oder externe Verursacher haben immer wieder deutlich gezeigt, dass Firmen dieser Verantwortung nicht oder nur ungenügend nachkommen können. Der kommerzielle Nutzen der Kommunikationsdaten sollte in diesem Zusammenhang nicht unterschätzt werden – nicht nur für Firmen im IT/TK-Umfeld.

Art. 25 Durchführung der Überwachung

Berufsgeheimnisträger

In ***Art. 25 Abs. 2*** wird die widerrechtliche Speicherung von Kommunikationsdaten und -inhalten für den Fall erzwungen, dass die Überwachung einer bestimmten Person auf Grund ihres Berufsstandes ohne besondere Ausnahmegenehmigung nicht möglich ist und diese Ausnahmegenehmigung nicht vorliegt.

Die Formulierung, „der Dienst zeichnet die Daten auf und benachrichtigt die Genehmigungsbehörde“ schreibt einen nicht zumutbaren Zustand für die betroffene

Person und den ISP fest, der die Daten an den Dienst liefern muss. Es wird an keiner Stelle darauf verwiesen, in welchem Zeitraum die nachträgliche Genehmigung zu erteilen ist noch was mit den Daten (und daraus vielleicht schon gewonnener Kenntnisse) passiert, wenn die Genehmigung nicht erteilt wird.

Ausserordentliche Überwachung

In ***Art. 25 Abs. 5*** wird auf „*Überwachungsmassnahmen, die nicht explizit in dieser Verordnung aufgeführt sind*“ verwiesen. In diesem Fall wird der gesamte „*Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen*“. Nähre Modalitäten dieser Überwachungsform werden in den Änderungen nicht beschrieben, sondern „*vom Dienst geregelt*“.

In den Erklärungen des erläuternden Berichtes[7] zu den geplanten Änderungen an der VÜPF wird hier mit der „in Anlehnung an die jahrelange durch Gerichte gestützte Praxis“ argumentiert. Wenn tatsächlich Gerichte heute schon Überwachungsmass-nahmen verfügen, die nicht durch die VÜPF abgedeckt sind, stellt sich uns die Frage, auf welcher gesetzlichen Grundlage diese Anordnungen erlassen werden und warum es dann überhaupt Regelungen für Echtzeit-Überwachungen durch eine VÜPF braucht?

Art. 27 Auskünfte über Internet-Teilnehmerinnen und -Teilnehmer

In ***Art. 27 Abs. 1*** werden die ISPs verpflichtet, dem Dienst verdachtsunabhängig und ohne weitere Anordnungen oder Genehmigungen Informationen über ihre Internet-Kunden auszuhändigen.

Aus unserer Sicht kann eine solche Anfrage nur nach Genehmigung durch eine zuständige Behörde zulässig sein. Die Informationen, die der Dienst von den ISPs im Rahmen dieser Verordnung einfordern darf, können sehr schnell die Privatsphäre von Personen berühren, die als unbeteiligte Dritte nicht legitimes Ziel einer Überwachungsmassnahme sind oder werden dürfen.

Kritik zu Artikeln in anderen Abschnitten

Art. 8 Verarbeitungszentrum

Datensicherheit

Die VÜPF sieht vor, dass der zuständige Dienst im EJPD ein Verarbeitungszentrum für die Daten aus der Überwachung des Fernmeldeverkehrs einrichtet. Die im Zentrum archivierten Daten werden rund um die Uhr denjenigen Behörden zugänglich gemacht, die als Empfängerinnen der Überwachungsdaten vorgesehen sind.

Eine zentrale Speicherung der durch Überwachung gewonnen sensiblen Daten ist aus Sicht des CCCZH indiskutabel, da jedes System für internen oder externen Verlust von Daten anfällig ist, der weder durch technische noch organisatorische Massnahmen

7 http://www.bfm.admin.ch/content/dam/data/pressemitteilung/2011/2011-06-08/110608_ber-de.pdf

vollständig verhindert werden kann (siehe dazu auch Anmerkungen zum ***Art. 24b***).

Einsicht in nicht-öffentliche Verzeichnisse

Der Dienst führt schliesslich für die Strafverfolgungsbehörde ein System zur Vermittlung von Auskunftgesuchen über Fernmeldeanschlüsse ein. Dieses System wird besonders die Erteilung von Auskünften über Anschlüsse ermöglichen, die in den öffentlichen Verzeichnissen der Fernmeldeanbiter nicht zu finden sind (siehe auch ***Art. 27***).

Dies gilt es aus Sicht des CCCZH konsequent abzulehnen. Es ist nicht nachvollziehbar zu erkennen, welche vermuteten Straftaten eine Einsichtnahme in diese Informationen und somit einen massiven Eingriff in die Privatsphäre rechtfertigen, d.h. ob beispielsweise ein einfacher Verdacht auf Steuerbetrug dafür ausreicht.

Art. 9 Datensicherheit

Nach ***Art.9 Abs. 2*** sind die Anbieterinnen von Kommunikationsdienstleistungen bei den Anordnungen zur Überwachung für die Datensicherheit der Überwachungsdaten bis zur Übergabe an den Dienst selbst verantwortlich.

Die zu ***Art. 24b*** geäusserte Kritik, dass keine technische oder organisatorische Massnahme den Verlust der Daten vollständig verhindern kann, gilt hier ohne Einschränkung.

Da zusätzlich nach ***Art. 2 Abs. 2 Bst. c*** des Datenschutzgesetzes[8] der Datenschutz für die Daten aus einer Überwachung nicht anwendbar ist, wird die nicht-intentionale Nutzung der Daten durch den Anbieter (zum Beispiel für eigene kommerzielle Interessen) nicht explizit ausgeschlossen. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Art. 17 Abs. 2 Berufsgeheimnisträger

Die zum ***Art. 25 Abs. 2*** geäusserte Kritik gilt auch für die entsprechenden Artikel in Bezug auf (Festnetz- und Mobil-)Telefonie. Interessanterweise gilt die Regelung, den speziellen Schutz der Kommunikation von Berufsgeheimnisträger bei einer Überwachung ohne spezielle Genehmigung zu ignorieren, nicht für den (physikalischen) Postverkehr.

Abschliessende Betrachtungen

Abschliessend ist aus Sicht des CCCZH folgendes festzustellen:

1. Bei der ***Echtzeitüberwachung*** kann *ohne Einschränkung*, d.h. ohne an die konkreten Vorgaben dieser Verordnung oder des zugrunde liegenden Bundesgesetzes gebunden zu sein, der gesamte Telefonie- und Internetverkehr einer verdächtigen Person auf Anordnung überwacht und gespeichert werden (***Art. 25 Abs. 5***). Dieses Vorgehen unterliegt dabei offensichtlich *keiner Kontrolle* durch

8 SR **235.1**

unabhängige Stellen, sondern obliegt allein der genehmigenden Behörde bzw. dem zuständigen Dienst beim EJPD. Auch die Regelungen zur *Überwachung von Berufsgeheimnisträgern ohne spezielle Genehmigung* ist unserer Meinung nach eine untragbare Regelung (***Art. 25 Abs. 2***). Dies mit einer „jahrelangen Praxis“ zu rechtfertigen, scheint aus Sicht des CCCZH fragwürdig und ist deshalb insgesamt konsequent abzulehnen.

2. Bei der ***rückwirkenden Überwachung (Vorratsdatenspeicherung)*** wird durch unpräzise Formulierungen (***Art. 24***) einer *Totalüberwachung* aller Internetnutzer durch *Protokollierung aller Internet-Aktivitäten* bei Dienste-Anbieterinnen Tür und Tor geöffnet. Die sich dadurch zwangsläufig ergebende Profilerstellung und der unkontrollierbaren Nebennutzung dieser Informationen ist aus Sicht des CCCZH mit der informationellen Selbstbestimmung nicht zu vereinbaren und deshalb konsequent abzulehnen.

Für die Beachtung unserer Kritikpunkte danken wir Ihnen bestens.

Mit freundlichen Grüssen,

Bernd Fix, i.A.d. Chaos Computer Clubs Zürich

Digitale Gesellschaft
c/o Swiss Privacy Foundation
5620 Bremgarten AG

Digitale Gesellschaft , c/o Swiss Privacy Foundation, 5620 Bremgarten AG

Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Bereich Recht und Controlling
Patrick Schöpf
3003 Bern

26. Juli 2011

Stellungnahme der Digitalen Gesellschaft zur geplanten Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrter Herr Schöpf
Sehr geehrte Damen und Herren

Von der geplanten Erweiterung des persönlichen und sachlichen Geltungsbereichs der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sind mehr Kreise betroffen, als der erläuternde Bericht beschreibt. Leider wird die aktuelle Vorlage auch der versprochenen Rechtssicherheit nicht gerecht.

Die unterzeichnenden Organisationen fühlen sich im weiteren Sinne der kritischen, digitalen Zivilgesellschaft verpflichtet. Wir erlauben uns daher, unsere Bedenken in einer gemeinsamen Stellungnahme darzulegen.

Zusammenfassung:

Die Digitale Gesellschaft lehnt den aktuellen Entwurf ab und fordert, dass der persönliche Geltungsbereich weiterhin auf professionelle Access Provider beschränkt bleibt und eine möglichst genaue Umschreibung der zulässigen Überwachungsmassnahmen mit der nächsten Überarbeitung des BÜPF im Gesetz festgeschrieben wird. Die Vorratsdatenspeicherung stellt einen schwerwiegenden Eingriff in die verfassungsmässig garantierten Grundrechte dar und bedarf daher einer klaren rechtlichen Grundlage. Eine Annahme der geplanten Änderungen schafft weder Rechtssicherheit noch „Investitionsschutz", wie es die Vorlage verspricht, sondern eliminiert sie geradewegs.

Digitale Gesellschaft
c/o Swiss Privacy Foundation
5620 Bremgarten AG

Kontakt:
office@digitale-gesellschaft.ch
www.digitale-gesellschaft.ch

Wir danken für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Piratenpartei Schweiz

Denis Simonet
Präsident

Swiss Internt User Group (SIUG)

Matthias Geiser
Aktuar

Swiss Privacy Foundation

Erik Schönenberger
Präsident

Verein Digitale Allmend

Hartwig Thomas
Vorstand

Verein „grundrechte.ch“

Viktor Györffy
Präsident

Anlage(n): Kurzvorstellung der unterzeichnenden Organisationen
Anhörungssantwort
(zugestellt per Post und E-Mail)

Kurzvorstellung der unterzeichnenden Organisationen

Die *Digitale Gesellschaft* versteht sich als ein offener Zusammenschluss netzpolitisch interessierter Gruppen und Einzelpersonen. Dazu gehören Grundrechtsorganisationen, Parteien, KünstlerInnen-Kollektive, BetreiberInnen von Netzwerkdiensten und weiteren Gruppen, die sich der kritischen, digitalen Zivilgesellschaft verpflichtet fühlen. (www.digitale-gesellschaft.ch)

Die *Piratenpartei Schweiz* vertritt die politischen Interessen der „digitalen Generation" und nimmt auf die politische Landschaft und Meinungsbildung Einfluss. Die Ziele der Piraten umfassen die Förderung des freien Zugangs zu Wissen und Kultur, die Stärkung der Bürgerrechte und der Privatsphäre, einen transparenten Staat und die Bekämpfung von Medienverboten und Zensur. Die am 12. Juli 2009 gegründete Partei zählt bereits über 1400 Piraten. (www.piratenpartei.ch)

Die *SIUG* ist eine Non-Profit-Organisation und Initiative der /ch/open, die sich aus Internet-Experten verschiedener Stufen zusammensetzt. Dazu gehören Akademikerinnen aus verschiedenen Fachgebieten, Experten aus dem IT Security-Bereich, selbständige Informatikerinnen und Anwender. Das Ziel der SIUG ist es, sich für eine vernünftige Anwendung, Entwicklung und Reglementierung des Internets und verwandter Technologien einzusetzen, wobei der ursprüngliche offene Geist und die Tradition des Mediums nicht übermässig eingeschränkt werden sollen. (www.siug.ch)

Die *Swiss Privacy Foundation* ist eine gemeinnützige Organisation, welche sich für den Schutz der digitalen Privatsphäre, für Meinungs- und Versammlungsfreiheit und den ungehinderten Informationszugang einsetzt. Zu ihren Mitgliedern zählen Akademikerinnen aus verschiedenen Fachgebieten, Computer- und Netzwerksicherheits-Experten, Juristinnen, selbständige Informatiker und Anwenderinnen. (www.privacyfoundation.ch)

Der *Verein Digitale Allmend* setzt sich dafür ein, den öffentlichen Zugang zu digitalen Gütern und deren Weiterentwicklung zu sichern. Er schafft neue Räume und fördert das öffentliche Verständnis für eine offene (Wissens-)Gesellschaft. (www.allmend.ch)

Der *Verein „grundrechte.ch"* wurde im Herbst 2006 als Nachfolgeorganisation der Stiftung Archiv Schnüffelstaat Schweiz (ASS) gegründet, welche im Anschluss an die Fichenaffäre entstanden ist. „grundrechte.ch" setzt sich für den Erhalt und den Ausbau der Grundrechte in der Schweiz ein. Schwerpunkt der Arbeit des Vereins ist der Schutz vor staatlicher Überwachung. (www.grundrechte.ch)

Stellungnahme zur geplanten Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)

Digitale Gesellschaft

unterzeichnet von den Organisationen
Piratenpartei Schweiz
Swiss Internet User Group (SIUG)
Swiss Privacy Foundation
Verein Digitale Allmend
Verein «grundrechte.ch»

26. Juli 2011

Zusammenfassung

Die Digitale Gesellschaft lehnt den aktuellen Entwurf ab und fordert, dass der persönliche Geltungsbereich weiterhin auf professionelle Access Provider beschränkt bleibt und eine möglichst genaue Umschreibung der zulässigen Überwachungsmassnahmen mit der nächsten Überarbeitung des BÜPF im Gesetz festgeschrieben wird. Die Vorratsdatenspeicherung stellt einen schwerwiegenden Eingriff in die verfassungsmässig garantierten Grundrechte dar und bedarf daher einer klaren rechtlichen Grundlage. Eine Annahme der geplanten Änderungen schafft weder Rechtssicherheit noch „Investitionsschutz", wie es die Vorlage verspricht, sondern eliminiert sie geradewegs.

1 Persönlicher Geltungsbereich

Der Begriff „Internet-Anbieterin" aus dem Gesetz soll gemäss den Erläuterungen angepasst werden. Sind bis anhin Access Provider gemeint, müsse das Gesetz nun generell für Anbieterinnen von Internetdienstleistungen gelten - um weiterhin eine effiziente Strafverfolgung zu gewährleisten. Skype, Chat, Instant Messaging, Internet-Telefonie etc. sollen laut Bericht überwachbar werden. Wo neu die Grenze zur Mitwirkungspflicht zu liegen kommt, wird aber nicht weiter erklärt. Ist ein von einem Verein betriebener, öffentlicher Chat-Server betroffen? Ein Web-Forum? E-Mails, die an eine Organisation über ein Kontakt-Formular auf der Homepage zugestellt werden? Eine Bibliothek, welche ihren BesucherInnen einen WLAN-Zugang zur Verfügung stellt? Eine Video-Botschaft, die bei Youtube veröffentlicht wird? Generell Anbieterinnen und/oder Server im Ausland?

Tatsächlich erhält in der Verordnung selber der Begriff „Internet-Anbieterin" keine neue Definition! Er lehnt sich im geltenden Recht wie auch im Entwurf an den Begriff „Fernmeldedienstanbieterin" an. Gemäss Fernmeldegesetzgebung gehört dazu eine fernmeldetechnische Übertragung „von Informationen über Leitungen oder Funk". Dies benötigt Leitungen oder Funkequipment: Betrifft also genau diejenigen, die Zugang zum Internet anbieten (oder die Netze untereinander verbinden) - jedoch nicht die Betreiberin eines Chat-Servers.

Die französische Fassung der Verordnung ist dann auch etwas genauer: Sie gilt aktuell für „Fournisseurs d'accès à Internet". Der Geltungsbereich der überarbeiteten Verordnung soll nun nicht mehr die Access Provider umfassen, sondern auf alle „Fournisseurs Internet" ausgeweitet werden - obwohl das übergeordnete Gesetz noch immer „nur" die „Fournisseurs d'accès à Internet" in die Pflicht nimmt!

Der erläuternde Bericht zur hängigen Totalrevision des BÜPF aus dem Jahr 2010 hält auch fest: „Der persönliche Geltungsbereich des BÜPF muss genauer formuliert und ergänzt werden. Denn neben den Anbieterinnen von Post- oder Fernmeldediensten, einschliesslich der Internet-Anbieterinnen (Zugangsvermittlerinnen, Access-Provider), können auch weitere Personen zu bestimmten Zeitpunkten Kommunikationsdaten besitzen, die die Strafverfolgungsbehörden bei der Bekämpfung der Kriminalität interessieren könnten." Und im entsprechenden Gesetzesentwurf wurde der Geltungsbereich dann auch über die „Internet-Anbieterinnen" (Art. 2 Abs. 1a) hinaus auf „Personen, die berufsmässig für Personen nach Buchstabe a Kommunikationsdaten verwalten, an Dritte Kommunikationsdaten weiterleiten oder die dafür notwendige Infrastruktur zur Verfügung stellen" (Abs. 1b) erweitert.

Diese geplante Neuregelung wurde in verschiedenen Vernehmlassungsantworten stark kritisiert. Wären damit doch sämtliche Firmen und Personen in einem kompletten Wirtschaftszweig zur Überwachung ihrer Kunden, Anschaf-

fung des entsprechenden Equipments und Abstellung von Personalressourcen verpflichtet. Bei der Einführung des BÜPF im Jahre 2000 wurden Randdaten, welche Telefon- und Internet-Zugangsanbieterinnen zum Zwecke der Rechnungsstellung und im Falle von Reklamationen über zu hohe Rechnungen ohnehin speicherten, dem Zugriff durch Strafverfolgungsbehörden zugänglich gemacht. Neu sollten sämtliche Anbieterinnen von Dienstleistungen im und um das Internet vorsorglich Investitionen für Überwachungsbegehren des Staates tätigen, die sie unter Umständen gar nie betreffen. Brancheninsider gehen davon aus, dass diese finanzielle Belastung für hunderte kleiner Betriebe das Aus bedeuten würde. Es gilt vom Gesetzgeber nicht nur die Wünsche der Strafverfolgungsbehörden zu berücksichtigen, sondern auch der marktwirtschaftlichen Realität ins Auge zu blicken.

Die Erläuterungen versprechen Rechtsunsicherheiten zu beseitigen. Durch die unklare Neuinterpretation des Begriffs „Internet-Anbieterin" schafft sie jedoch neue. Dabei werden nach Gutdünken der Überwachungsbehörden Befugnisse erweitert und Grundrechte beschnitten. Das Ziel hingegen, z.B. ein Skype-Gespräch abhören zu können, wird nicht erreicht. Um diese verschlüsselten Gespräche abhören zu können, müsste auf den zu überwachenden PCs eine Schnüffelsoftware (Trojaner Federal) installiert werden. Eine entsprechende Zwangsmassnahme war mit der Verschärfung der Strafprozessordnung im Rahmen der letztjährigen Revision des BÜPFs vorgesehen. Sie ist technisch wie rechtlich (international) stark umstritten - und dementsprechend im Vernehmlassungsverfahren auf breite und entschiedene Ablehnung gestossen.

Die Digitale Gesellschaft befürwortet eine eindeutigere Definition des persönlichen Geltungsbereichs des BÜPF. Die Bestimmungen haben jedoch im Bereich Internetüberwachung weiterhin nur für professionelle Access Provider zu gelten. Eine zu überwachende Person muss da, wo sie ist, also bei der lokalen Zugangsanbieterin, überwacht werden. Nur diese befindet sich, schon von ihrer Natur her, zwingend in der Schweiz und untersteht schweizerischem Recht. Die überwiegende Mehrheit der anderen Dienstanbieterinnen operieren hingegen aus dem Ausland; sei es nun Skype, Gmail, GMX oder Facebook. Die Bestimmungen greifen somit auch nur bei einem Bruchteil von ihnen, erwirken bei den inländischen Firmen durch die zusätzlichen Kosten (Anschaffung des entsprechenden Equipments und Abstellung von Personalressourcen) jedoch einen beträchtlichen Wettbewerbs- und der Schweiz einen Standortnachteil.

2 Sachlicher Geltungsbereich

Die zweite weitreichende Änderung betrifft die Überwachungstypen. Bis anhin sind die Kommunikations-Arten, für welche eine Überwachung angeordnet werden kann, in der Verordnung abschliessend aufgeführt. Diese Auffassung wird auch vom Bundesverwaltungsgericht vertreten.

In der Praxis scheinen sich Untersuchungsbehörden und Zwangsmassnahmengerichte jedoch über den Wortlaut hinwegzusetzen und weitergehende Überwachungen zu veranlassen. Tatsächlich hat auch der Dienst „Überwachung Post- und Fernmeldeverkehr" bereits 2009 technische Richtlinien erlassen, welche die Provider dazu zwingen, Massnahmen zu ergreifen, welche die Echtzeitüberwachung des kompletten Internetdatenverkehrs ermöglichen. Verhängnisvollerweise wurde den Providern vom Bundesgericht (BGE 130 II 249) die Möglichkeit genommen, die Rechtmässigkeit einer Überwachungsanordnung an sich zu bestreiten.

Bisher betreffen die Überwachungstypen bezüglich dem Internet (Art. 24) den E-Mail-Verkehr und das Einwählen ins Internet. Mit der aktuellen Neuregelung sollen WLAN, grundsätzlich „elektronische Postdienste", Multimediadienste(!?) etc. dazukommen. Und nicht mehr „nur" für Internetzugänge gelten sondern auch für „andere Internetanwendungen". Es wird sogar verordnet, dass die Aufzählung als nicht abschliessend zu betrachten sei - und dass selbst der komplette Datenverkehr in Echtzeit und permanent zum Verarbeitungszentrum im EJPD übertragen werden muss.

Damit vollzieht sich ein grundsätzlicher Wechsel in der Interpretation des Gesetzes. Es sollen nicht mehr „nur" Gespräche, E-Mails und Einwähldaten zur Verfügung gestellt werden müssen - sondern sämtliche Daten (und in Echtzeit), die von und zu einem Anschluss fliessen: Surfen im Netz, Recherchieren bei Google, Newsabfrage bei 20min.ch, virtueller Kinobesuch auf Youtube, Updates des Betriebssystems etc. pp. Dies stellt einen beträchtlichen (zusätzlichen) Eingriff in die persönlichen Freiheiten dar, und stellt nicht nur die Provider vor grössere Herausforderungen und Anschaffungen, sondern auch den Dienst selbst.

Eine derart massive Erweiterung des sachlichen Geltungsbereichs hat zwingend auf Gesetzesebene zu erfolgen. Auch bei der Erarbeitung des Vorentwurfs zur Revision des BÜPF wurde diese Notwendigkeit erkannt und in Art. 21 eine entsprechende Anpassung des heutigen Art. 15 BÜPF vorgeschlagen.

Die Digitale Gesellschaft befürwortet eine klare Definition der Datenarten, welche im Rahmen einer Überwachung angeordnet werden können. Diese müssen jedoch auf Gesetzesstufe festgehalten werden. Entsprechende Schranken sorgen für die gebotene Rechtssicherheit bei den Providern (und Bürgern) und für den versprochenen „Investitionsschutz". Sie müssen auch von den Strafverfolgungsbehörden und vom Dienst ÜPF eingehalten werden. Die Datenarten sind als „E-Mail", „Telefongespräche (auch über das Internet)", „Textnachrichten (wie SMS)" etc. festzuhalten. Sie dürfen jedoch nicht pauschal „den gesamten Datenfluss" betreffen.

Die Provider müssen zudem die Rechtmässigkeit einer Überwachungsanordnung gerichtlich feststellen lassen können. Auch dies dient der Rechtssicherheit aller Beteiligter. Die Interpretation des Gesetzes und der Verordnung kann nicht allein dem Dienst und den zuständigen Stellen für die Strafverfolgung

überlassen werden. Die Rekursmöglichkeit ist im Gesetz festzuhalten.

3 Vorratsdatenspeicherung

Die geplanten Erweiterungen des persönlichen und sachlichen Geltungsbereichs betreffen ebenfalls die Vorratsdatenspeicherung. Auch dabei soll die Aufzählung der (Kommunikations-)Parameter in der Verordnung nicht mehr abschliessend gelten.

Zur Erinnerung: Es geht hier nicht, wie es der verharmlosende Begriff suggeriert, um eine „rückwirkende Überwachung". Vielmehr handelt es sich um eine flächendeckende und verdachtsunabhängige Überwachung von sämtlichen NutzerInnen von Telefon-, E-Mail- und Internetdiensten - mit der Absicht, die Daten bei Bedarf gezielt auswerten zu können. Dies stellt einen schwerwiegenden Eingriff in die verfassungsmässig garantierten Grundrechte dar - und muss daher gemäss Bundesverfassung im Gesetz selbst und nicht etwa in einer Verordnung geregelt sein.

Sämtliche Verfassungsgerichte (Deutschland, Irland, Bulgarien und Rumänien), welche die nationale Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung bis anhin zu beurteilen hatten (und in etwa der schweizerischen Regelung entspricht), haben sie als nicht verfassungsmässig eingestuft. In Deutschland wurde gar die unverzügliche Löschung der bis anhin gesammelten Daten angeordnet. Viele sind der Ansicht, dass die Vorratsdatenspeicherung gegen die Menschenrechte verstossen würde, da der nach Artikel 8 der Europäischen Menschenrechtskonvention zu wahrende Verhältnismässigkeitsgrundsatz - beim Eingriff ins Recht auf Achtung des Privat- und Familienlebens - nicht erfüllt sei.

Gemäss den Erläuterungen zum aktuellen Entwurf sind unter den zu protokollierenden „Datenverbindungen" die Internet-Sessions zu verstehen und nicht jede einzelne Aktion innerhalb einer solchen Session. Um eine Identifikation der Internet-BenutzerInnen vornehmen zu können, reichen diese Informationen jedoch nicht aus, wenn die IP-Adresse von der Anbieterin übersetzt wird und sich mehrere User eine öffentliche IP-Adresse teilen. Diese Technik zur Network Address Translation (NAT) kommt bei Zugängen via WLAN und Mobilfunk in den meisten Fällen zur Anwendung. Leider fehlt in der Verordnung die Definition der „Datenverbindung". Es steht zu befürchten, dass der Spielraum sehr bald genutzt wird, um entsprechende weitergehende technische Richtlinien zu erlassen. Werden heute IP-Zuordnungen vorgehalten, müssten neu sämtliche IP-/Netzwerkverbindungen protokolliert werden. Diese bilden das umfassende Nutzerverhalten im Internet ab. Entsprechend notwendige Bestimmungen zu Datenschutz und Datensicherheit fehlen.

Bitte beachten Sie die ausführliche Stellungnahme zur Vorratsdatenspeicherung in der Vernehmlassungsantwort zur Totalrevision des Bun-

desgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) der Swiss Privacy Foundation vom 16. August 2010 (Kapitel 8, http://www.privacyfoundation.ch/vernehmlassungsantwort_20100816.pdf).

Die Digitale Gesellschaft sieht die Verhältnismässigkeit bei einer anlassunabhängigen Vorratsdatenspeicherung nicht gegeben. Falls auf diese rechtsstaatlich bedenkliche Massnahme nicht verzichtet werden kann, muss sie unter strengsten Auflagen vorgenommen werden. Die Personen und Daten, welche betroffen sind, müssen genau bezeichnet und auf möglichst wenige beschränkt sein. Sie müssen im Gesetz selber und nicht etwa in einer Verordnung geregelt sein. Die Deutungshoheit darf nicht den Strafverfolgungsbehörden oder dem Dienst ÜPF überlassen werden.

4 Schlussbetrachtung

Dass das Internet mehr und mehr die analoge Fernmeldetechnik verdrängt, ist offensichtlich. Der Forderung nach weiteren Überwachungsbefugnissen würde es aber gut zu Gesicht stehen, wenn die fehlenden Möglichkeiten (zur Strafverfolgung von „Extremismus"?!) genauer erläutert und die geforderten Befugnisse konkreter begründet würden. Aus den vorliegenden Erläuterungen kann jedoch nicht auf eine angeblich gebotene Dringlichkeit geschlossen werden, die ein Überholen der hängigen Totalrevision rechtfertigen würde - anstatt diese zu beschleunigen. Vielmehr lassen sie die Vermutung zu, dass mit der Änderung bereits vollendete Tatsachen geschaffen werden möchten, resp. gängige Praxis in Recht zu überführen versucht wird - und dass die Totalrevision zu stark umstritten ist, als dass mit einer baldigen Inkraftsetzung zu rechnen ist.

Die Digitale Gesellschaft anerkennt das Bedürfnis nach einer effizienten Verbrechensaufklärung. Sie muss aber rechtsstaatlichen Prinzipien genügen. Je schwerer ein Eingriff in die Freiheitsrechte wiegt, desto genauer muss er im entsprechenden Gesetz vorgesehen sein. Dies ist Voraussetzung, um für Rechtssicherheit zu sorgen. Mit nicht abschliessenden Aufzählungen ist dieses Ziel nicht zu erreichen. Zudem muss die Massnahme zweckmässig und verhältnismässig sein.

Vor diesem Hintergrund erstaunt es, dass der persönliche und sachliche Geltungsbereich auf dem Verordnungsweg im dargestellten Umfang erweitert werden soll. Beide Bereiche sind immer auch im direkten Zusammenhang zu sehen. Wird ein Verein, der einen öffentlicher Server für Instant Messages betreibt, dem persönlichen Geltungsbereich des BÜPF unterstellt, muss er auch den sachlichen Geltungsbereich erfüllen und selbst die Vorratsdatenspeicherung, also die (rückwirkende) Identifzierung seiner Nutzer, gewährleisten.

Der Hotelier, der seinen Gästen WLAN anbietet, kann dies eigentlich nur, indem er den kompletten Datenverkehr aufzeichnet und für 6 Monate aufbewahrt. Da sich seine Kunden zum Internet hin eine IP-Adresse teilen, kann nur

so zweifelsfrei festgestellt werden, welcher Gast sich zum gefragten Zeitpunkt, auf dem spezifizierten Server im entsprechenden Web-Forum aufgehalten hat. Diese Pflicht kann vom Gesetzgeber kaum gewollt sein.

Die Digitale Gesellschaft lehnt den aktuellen Entwurf ab und fordert, dass der persönliche Geltungsbereich weiterhin auf professionelle Access Provider beschränkt bleibt und eine möglichst genaue Umschreibung der zulässigen Überwachungsmassnahmen mit der nächsten Überarbeitung des BÜPF im Gesetz festgeschrieben wird. Die Vorratsdatenspeicherung stellt einen schwerwiegenden Eingriff in die verfassungsmässig garantierten Grundrechte dar und bedarf daher einer klaren rechtlichen Grundlage. Eine Annahme der geplanten Änderungen schafft weder Rechtssicherheit noch „Investitionsschutz", wie es die Vorlage verspricht, sondern eliminiert sie geradewegs.

economiesuisse

Informatik Service Center ISC-EJPD
Dienst Überwachung Post- und
Fernmeldeverkehr
Bereiche Recht und Controlling
Patrick Schöpf
3003 Bern

7. Juli 2011

VÜPF Änderungsvorlage vom 8. Juni 2011

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit im Rahmen der Revision der Verordnung fristgerecht über die Überwachung im Post- und Fernmeldewesen Stellung zu nehmen. Wir erlauben uns folgende Punkte aufzugreifen:

- Aus unserer Sicht handelt es bei der Revision um eine Verankerung neuer Überwachungsmassnahmen, wie die umfassende Überwachung des Internen Verkehrs. Ausserdem werden neue Massnahmen eingeführt, die mit grosser Wahrscheinlichkeit keine Rechtsgrundlage haben, wie z.B. Antennensuchläufe. Bei Antennensuchläufen bestehen keine konkreten Verdachtsmomente gegen Personen oder Anschlüsse wie dies vom Gesetzgeber gefordert wird. Auf diese Weise wird die Rechtssicherheit nicht aus- sondern abgebaut.
- Die angeführte Kostensenkung trifft nicht zu: Vielmehr handelt es sich um eine Umlagerung der Kosten von den Verursachern hin zur Allgemeinheit. Es ist davon auszugehen, dass mit dieser Anpassung die Gesamtkosten aus volkswirtschaftlicher Sicht sogar deutlich steigen werden – seitens Überwachungsbehörden wird Tür und Tor für eine weitreichende Überwachungspraxis geöffnet, ohne, dass die Kosten von den Behörden getragen werden müssen.
- Vom materiellen Gehalt her haben wir es bereits mit einer Totalrevision der VÜPF zu tun, auch wenn diese als Teilrevision angepriesen wird. Die Revision soll Entscheidungen vorwegnehmen, welche eigentlich in den Rahmen der BÜPF Revision gehören.

Aus den genannten Überlegungen möchten wir sie bitten, die Revision der VÜPF nicht weiter zu verfolgen, sondern zunächst die Revision des BÜPF abzuschliessen und die Verordnungsrevision im Nachgang zur Gesetzesrevision zu vollziehen.

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

Für weitere Rückfragen stehen wir gerne zu Ihrer Verfügung.

Freundliche Grüsse
economiesuisse

Dominique Reber
Mitglied der Geschäftsleitung

Dr. Meinrad Vetter
Stv. Leiter Wettbewerb und Regulatorisches