Vernehmlassungsantwort zur Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Swiss Privacy Foundation,
mitunterzeichnet von der
Swiss Internet User Group (SIUG)

16. August 2010

Zusammenfassung

Die Swiss Privacy Foundation steht der geplanten Totalrevision des BÜPF kritisch gegenüber. Der vorgelegte Entwurf ist ungenau und schiesst weit über das Ziel hinaus. Dem verfassungsmässig garantierten Schutz der Privatsphäre und der Verhältnismässigkeit hinsichtlich des technischen und finanziellen Aufwands wird nicht angemessen Rechnung getragen.

Inhaltsverzeichnis

1 Persönlicher Geltungsbereich

Gemäss dem unterbreiteten Vorentwurf soll der persönliche und sachliche Geltungsbereich des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) beträchtlich erweitert werden.

Das aktuell gültige Gesetz betrifft „alle staatlichen, konzessionierten oder meldepflichtigen Anbieterinnen von Post- und Fernmeldedienstleistungen sowie Internet-Anbieterinnen“ (Art. 1 Abs. 2). Damit sind gemäss dem erläuternden Bericht zur Änderung des BÜPF (Seite 17 Abs. 1) Zugangsvermittlerinnen (sogenannte Access Provider) gemeint, welche dem Fernmeldegesetz unterstehen und somit gemäss Leitfaden zum Fernmeldegesetz „Informationen für Dritte fernmeldetechnisch selber übertragen oder übertragen lassen und diesen Dritten gegenüber im Rahmen eines privatrechtlichen Vertragsverhältnisses die Verantwortung für die Erbringung der versprochenen Dienstleistung übernehmen“ (Punkt 1.2.5).

Somit fallen sämtliche professionellen Anbieterinnen von Internet-Zugängen unter den Geltungsbereich des BÜPF. In einer Analogie könnte man festhalten, dass dadurch bereits heute sämtliche Ein- und Ausfahrten der (Daten-)autobahn, auch inhaltlich, überwacht werden können.

Im Vorentwurf weicht diese Definition nun derjenigen aus Artikel 2 Abschnitt 1a, welche den Geltungsbereich auf „Anbieterinnen von Post- und Fernmeldediensten, einschliesslich Internet-Anbieterinnen, die ihre Tätigkeit berufsmässig ausüben“ ausdehnt. Leider wird darauf verzichtet, den Begriff „Internet-Anbieterinnen“ genauer zu definieren. Der erläuternde Bericht schreibt beispielshaft von „Webhostern (Service- und Hosting-Provider)“ und „elektronischen Postdiensten“. Gemeint sind also nicht mehr nur Access Provider, die dem Fernmeldegesetz unterstehen, sondern neu sämtliche „Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind“ (Wikipedia, Stichwort: Internetanbieter). Konkret trifft dies also auf alle Unternehmen zu, welche professionelle Leistungen für die Nutzung oder den Betrieb des Netzes im Bereich Datenvermittlung, Domain-, Server-, Web- und Mail-Hosting, Housing oder Anwendungen anbieten - und dürfte selbst für Content Provider gelten.

Damit wären sämtliche Firmen und Personen in einem kompletten Wirtschaftszweig zur aktiven Überwachung, Anschaffung des entsprechenden Equipments und Abstellung von Personalressourcen verpflichtet - und dies (wie weiter unten in Kapitel 4 festgehalten) auf eigene Kosten.

Darüber hinaus sollen alle, welche eine solche Tätigkeit nicht berufsmässig ausüben, angehalten sein, „Überwachungen nach dem Gesetz zu dulden“ (Art. 2), „den vom Dienst beauftragten Personen Zutritt zu den von ihnen verwendeten Einrichtungen zu gewähren“ und „die notwendigen Auskünfte [zu] erteilen“

(Art. 26).

Somit werden zusätzlich auch alle Privatpersonen, Organisationen und Unternehmen, welche Internetdienstleistungen nebenbei anbieten, zur passiven Mithilfe und zur Verfügungstellung ihrer Räumlichkeiten und Computereinrichtungen, wie Netzwerkgeräten und Servern, gezwungen. Dies kann sogar bedeuten, dass Passwörter und Verschlüsselungs-Keys bekanntgegeben werden müssen und unter Zuhilfenahme privater Gerätschaften Abhörmassnahmen durchgeführt werden können.

Im Vergleich wären nun alle Geschäfte und Restaurants entlang der (Daten-)autobahn dazu verpflichtet, Kameras und Mikrofone zu installieren und die daraus gewonnenen Daten der Strafverfolgungsbehörde im konkreten Fall zur Verfügung zu stellen. Und selbst die AnwohnerInnen müssten die Installation entsprechender Anlagen in ihren Räumlichkeiten dulden und die Überwacher wo nötig unterstützen.

Wie bereits erwähnt, sind alle Zugänge bereits heute mit dem aktuellen Gesetz überwachbar. Eine Ausdehnung der Zuständigkeit für die aktive Überwachung oder passive Mithilfe auf sämtliche Personen und Firmen, die Dienstleistungen Rund um das Internet anbieten oder Services im Netz zur Verfügung stellen, ist unverhältnismässig und nicht akzeptabel.

Dies auch darum, weil für sie ebenfalls der sachliche Geltungsbereich erweitert werden soll und zusätzliche Pflichten, z.B. im Bereich Zertifizierung, „Trojaner Federal“ oder der Vorratsdatenspeicherung, gelten sollen (in nachfolgenden Kapitel weiter ausgeführt).

E-Mails, SMS und Telefonate können mit dem gültigen Gesetz überwacht werden. Die Absicht des Gesetzgebers ist genügend ersichtlich, so dass unter Verweis auf die technische Entwicklung die Überwachungstypen (beschrieben in der gültigen Verordnung in Artikel 16) um die Internet-Telefonie ergänzt werden könnte.

Ausserdem gilt festzuhalten, dass sich die Zugangsanbieterinnen, schon von ihrer Natur her, zwingend in der Schweiz befinden müssen - und konzessionspflichtig sind. Sie unterstehen damit automatisch schweizerischem Recht. Die überwiegende Mehrheit der anderen Dienstanbieterinnen operieren jedoch aus dem Ausland; sei es nun Skype, Gmail, GMX oder Facebook. Das Gesetz greift somit nur bei einem Bruchteil von ihnen, erwirkt bei den inländischen Firmen durch die zusätzlichen Kosten jedoch einen beträchtlichen Wettbewerbs- und der Schweiz einen Standortnachteil.

Die Swiss Privacy Foundation begrüsst eine genauere Definition des Geltungsbereichs. Sie fordert jedoch, dass dieser weiterhin auf professionelle Internet-Zugangsanbieterinnen zu beschränken sei - und nicht auf Hostingprovider und Inhaltsanbieterinnen ausgedehnt wird. Für nicht berufsmässige Akteure soll weiterhin keine Mithilfe- und Auskunftspflicht bestehen. Das aktuel-

le Gesetz genügt, um den Strafuntersuchungsbehörden genügend Möglichkeiten zur Anordnung von strafprozessualen Zwangsmassnahmen, die zur Erfüllung ihrer Aufgaben nötig sind, zur Hand zu geben.

2 Überwachungstypen (Sachlicher Geltungsbereich)

In der aktuell gültigen Verordnung zum BÜPF sind in Artikel 16 die Typen, die im Bereich der Internetüberwachung angeordnet werden können, abschliessend geregelt. Diese betreffen Verkehrs- und Inhaltsdaten von E-Mails und Einwähldaten ins Internet. Mit einer Anpassung der Verordnung könnten bereits heute Telefonate, welche über das Internet geführt werden, legal überwacht werden.

Tatsächlich hat der Dienst „Überwachung Post- und Fernmeldeverkehr“ - ohne entsprechende rechtliche Grundlage gemäss VÜPF - bereits 2009 technische Richtlinien erlassen, welche die Provider dazu zwingen, Massnahmen zu ergreifen, welche die Echtzeitüberwachung des kompletten Internetdatenverkehrs ermöglichen. Mitte 2010 erhielten die 650 registrierten Fernmeldedienstanbieterinnen nun wiederum Post vom EJPD, mit welcher die Unternehmen vom Dienst darüber unterrichtet werden, dass der Bund in den kommenden Monaten diese Funktion, vorerst für E-Mails und Internet-Telefonie, mit jeder einzelnen Anbieterin testen will.

Anders als im erläuternden Bericht zur Vernehmlassung beschrieben, nämlich dass der Gegenstand des neuen BÜPF im Wesentlichen jenem des derzeitigen Gesetzes entsprechen würde, wird hier ein grundsätzlicher Wechsel vollzogen. Anstelle der abschliessenden Aufzählung von Überwachungstypen tritt im geplanten Gesetz der Artikel 21 Abschnitt 3, der die Weiterleitung vom „gesamten Datenfluss der überwachten Person“ an den Dienst festschreibt.

Es müssten also nicht mehr „nur“ Gespräche, E-Mails und Einwähldaten zur Verfügung gestellt werden, 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. - und dies nicht auf wohlstrukturierter Nachrichten- oder Gesprächsebene, sondern auf tiefem technischem Level inkl. sämtlicher „Steuersignale“, die zur Übertragung benötigt werden.

Dies stellt nicht nur die Provider vor grössere Herausforderungen und Anschaffungen, sondern auch den Dienst selbst. Um die komplexe Extraktion der wirklich relevanten Daten delegieren zu können, sorgt der zweite Teil des Artikels dafür, dass die Anbieterinnen „auf Verlangen des Dienstes [...] nur den bezeichneten Typ oder die bezeichneten Typen von Daten aus dem Datenstrom“ zu liefern haben. Auch hier werden private Unternehmen auf eigene Kosten zur Gehilfenschaft bei Strafuntersuchungen verpflichtet.

Ebenfalls wichtig ist, dass - wie oben in Kapitel Geltungsbereich festgehalten - nicht mehr „nur“ Access Provider, sondern neu sämtliche professionellen und in der Schweiz beheimateten Anbieterinnen von Dienstleistungen und Inhalten rund um das Internet angehalten werden sollen, derartige Überwachungen durchzuführen.

Die Swiss Privacy Foundation begrüsst eine klare Definition der Datenarten, welche im Rahmen einer Überwachung angeordnet werden können - auf Gesetzesstufe. Entsprechende Schranken sorgen für Rechtssicherheit bei den Providern und müssen 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.

3 Rekursmöglichkeiten

Gemäss Vorentwurf zum neuen BÜPF sollen die Rekursmöglichkeiten der Provider gesetzlich massiv eingeschränkt werden: „Mit der Beschwerde gegen die Verfügung des Dienstes kann die Rechtmässigkeit der Überwachung nicht geltend gemacht werden“ (Art. 34 Abs. 2).

Damit wird das Bundesgerichtsurteil 130 II 249 im Gesetz verankert. Dieses Urteil entzieht den Access Providern die Möglichkeit, die rechtliche Grundlage einer Überwachungsanordnung in Frage zu stellen. Das hat zur etwas absurden Situation geführt, dass einige Access Provider zähneknirschend (um Schlimmeres zu verhindern) sogar an der Ausarbeitung der technischen Richtlinien des Dienstes zur Überwachung des gesamten Internetdatenverkehrs mitgearbeitet haben.

Es steht nicht zu befürchten, dass ein Provider dieses Recht missbraucht, um eine Überwachungsanordnung mit einem (allenfalls teuren) Rechtsstreit zu verzögern oder zu umgehen. Es ist aber wichtig, dass allfällige Unklarheiten im Gesetz durch unabhängige Gerichte aufgrund von Rekursen geklärt werden können. Analog zu den Beschwerdemöglichkeiten im technischen und organisatorischen Umfeld, könnte auch dieser Bestimmung die aufschiebende Wirkung (bezüglich einer konkreten Überwachungsanordnung) entzogen werden.

Die Swiss Privacy Foundation fordert, dass betroffene Provider die Rechtmässigkeit einer Überwachungsanordnung gerichtlich feststellen lassen können. 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 Möglichkeit ist im Gesetz festzuhalten.

4 Kosten, Zertifizierung und Entschädigungen

Wie bis anhin müssen auch mit dem neuen Gesetz die Anbieterinnen für die Beschaffung der notwendigen Gerätschaften, welche die Überwachung ermöglichen, selber aufkommen. Sie sind verpflichtet, entsprechendes Personal auszubilden und abzustellen. Der Bundesrat kann vorsehen, dass eine Mitteilung „kostenlos und rund um die Uhr zu erfolgen hat".

Neu ist zusätzlich eine Zertifizierung der Anbieterinnen vorgesehen (Art. 18). Sie ist zwar nicht zwingend, jedoch müssen Anbieterinnen ohne entsprechende Bescheinigung „die Kosten tragen, die entstehen, wenn der Dienst oder Dritte einer angeordneten Überwachung beigezogen werden müssen. Tritt dieser Fall ein, müssen sie sich anschliessend so schnell wie möglich gemäss Artikel 18 zertifizieren lassen" (Art. 24).

Wie selbstverständlich wird hier der gesamte Wirtschaftszweig zusätzlich gezwungen, sich für die Strafuntersuchung fit zu machen und diese selbstständig für den Staat auszuführen. Wer sich nicht zertifizieren lässt, wird im Falle einer angeordneten Überwachung für unvorhergesehene (und nicht im Voraus bezifferbare) Kosten aufkommen müssen. Dies kann für viele Betriebe zu einem finanziell schwer zu verkraftenden Schaden führen. Die Anbieterinnen, welche die Zertifizierung durchlaufen, müssen möglicherweise gar nie eine angeordnete Überwachung ausführen. In diesem Fall würden die Kosten und Aufwand einem fehlenden Nutzen für die Strafverfolgung gegenüberstehen.

Unverständlich ist auch die geplante Abschaffung der bis anhin geltenden Entschädigungen (Art. 30 Abs. 1). Es gilt an der Stelle nochmals darauf hinzuweisen, dass dies neu für tausende Schweizer Firmen gelten soll: Für viele Kleinbetriebe, Internet Startups etc. dürften diese ungedeckten Aufwendungen existenzbedrohend sein.

Die Implementation einer Überwachungsinfrastruktur und der Abschluss der Zertifizierung sind wirtschaftlich gesehen eine Investition und somit eine mittel- bis längerfristige Belastung des operativen Geschäftes. Wer die Investition tätigt, erhält dafür jedoch keinen Nutzen und schafft keinen Mehrwert.

Der erläuternde Bericht versucht dies schönzureden und mit dem Effizienzgewinn bei der Strafverfolgung zu relativieren. Zudem würden „die Überwachungskosten nur einen geringen Teil ihres Umsatzes" ausmachen (Seite 51 Punkt 3.3). Das mag wohl richtig sein, doch genauso macht auch der Unternehmensgewinn meist nur einen geringen Teil des Umsatzes aus. Die Firmen aus der Internet-Branche agieren bereits seit einigen Jahren in einem gesättigten Markt, in dem ein massiver Preisdruck herrscht. Für die Anbieterinnen ist es bereits heute schon sehr schwierig geworden, profitabel zu sein. Es gilt nicht nur die Wünsche der Strafverfolgungsbehörden zu berücksichtigen, sondern auch der marktwirtschaftlichen Realität ins Auge zu blicken.

Interessant ist, dass die anordnende Behörde gegenüber dem Dienst jedoch

eine Gebühr zu entrichten hat (Art. 30 Abs. 2). Und der ergänzende Bericht zur Vernehmlassung gibt auch gleich eine Empfehlung, wie dieser Betrag gedeckt werden kann: „Als Verfahrenskosten bzw. als Auslagen [kann er] ganz oder teilweise Dritten, insbesondere der verurteilten oder beschuldigten Person auferlegt werden“ (Seite 38 Abs. 3).

In dieser Logik kommt neu nicht mehr der Staat für die Strafuntersuchung auf, sondern vielmehr soll diese nun von Privaten und auf Kosten der beschuldigten Person durchgeführt werden.

Eine Überwachung stellt einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. Die Bundesverfassung garantiert das Schrift- und Fernmeldegeheimnis. Die Überwachungspflicht im vorliegenden Umfang an Private zu delegieren ist nicht gerechtfertigt.

Es gilt zudem zu bedenken, dass eine vorhandene Infrastruktur von den beteiligten Firmen oder Einzelpersonen auch für eigene Zwecke missbraucht werden könnte. Der erläuternde Bericht schweigt sich leider darüber aus, wie dem angemessen entgegengewirkt werden könnte.

Die Swiss Privacy Foundation ist der Ansicht, dass die Durchführung von Strafuntersuchungen, insbesondere von Überwachungsmassnahmen, Sache des Staates ist. Dieser hat grundsätzlich auch dafür aufzukommen. Die bereits vorhandene Mitwirkungspflicht der Access Provider ist angemessen und reicht für die Strafuntersuchung aus. Die Kosten für die Überwachung ist den Providern wie bis anhin zu entschädigen. Auf eine Zertifizierung ist zu verzichten.

5 Voraussetzungen

Neu soll der Artikel mit der Aufzählung der strafbaren Handlungen, zu deren Verfolgung eine Überwachung angeordnet werden kann, in der Eidgenössischen Strafprozessordnung geführt werden. Der entsprechende Artikel 269 Abschnitt 2a wurde auch gleich um zwei Dutzend neue Straftatbestände erweitert, wie beispielsweise:

- Diebstahl
- Sachbeschädigung mit grossem Schaden
- Gewerbsmässiger Wucher
- In Umlaufsetzen falschen Geldes
- Falsche Anschuldigungen
- Bestechung

Festzuhalten ist, dass jener abschliessende Straftatenkatalog bereits heute nicht gilt, falls die Straftat über das Internet begangen worden ist: Es „müssen Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, dem Dienst alle Angaben machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen“ (VE Art. 20.3).

Die Swiss Privacy Foundation fordert, dass die Ausdehnung auf zusätzliche Anlassstraftaten kritisch hinterfragt wird. Zudem hat der Katalog auch für den Zugriff auf Daten aus der Vorratsdatenspeicherung („Rückwirkende Überwachung“, Identifizierungspflicht) zu gelten.

6 Trojaner Federal (Informatikprogramme zum Abfangen von Daten)

Was im Vorentwurf verharmlosend als „auch ohne Wissen der überwachten Person das Einführen von Informatikprogrammen in ein Datensystem anordnen, um die Daten abfangen und zu lesen“ (StPO Art. 270bis) umschrieben ist, bedeutet nichts geringeres als das heimliche Eindringen in ein fremdes Computersystem und das Installieren von Überwachungs- resp. Schadsoftware, welche normalerweise von einem Antiviren-Schild verhindert würde.

Folgerichtig sieht der ergänzende Bericht (Seite 42 Abs. 3) auch vor, dass ein zusätzliches Programm zur Umgehung des Antivirenprogramms eingeführt werden kann.

Diese Massnahme soll von aussen den Zugriff auf „beispielsweise Korrespondenz, Fotos, Filme, die zur Privat- oder sogar Intimsphäre gehören“ ermöglichen (Seite 43 Abs. 2). Sie ist sogar geeignet, das eingebaute Mikrofon und die Videokamera am überwachten PC fernzusteuern.

Die in der Überwachungsanordnung von der Staatsanwaltschaft anzugebenden Datenart hilft nicht, die Schwere des Eingriffs für die von der Überwachung betroffene Person zu reduzieren, da ohne einen entsprechenden Zugriff die Art nicht eindeutig bestimmt werden kann.

Dieses neue Recht bleibt nicht nur den Strafverfolgungsbehörden vorbehalten, sondern vielmehr werden auch hier die Provider zur „nötigen Unterstützung“ (Art. 21 Abs. 4) verpflichtet.

Um den Vorgang zu verdeutlichen, kann ein Vergleich aus der „analogen“ Welt herangezogen werden: Der lokale Schlüsseldienst hilft der Polizei beim unbemerkten Eindringen in eine Wohnung und beim Ausschalten der Alarmanlage. Das Haus wird von den BeamtInnen ohne ZeugInnen durchsucht - und Mini-Überwachungskameras und Wanzen werden angebracht. Damit ein Zugriff auf diese Geräte auch später und von aussen möglich bleibt, wird die Alarmanlage und Hintertüre entsprechend präpariert.

Dieser Vorgang wird in Deutschland unter dem Begriff „Online-Durchsuchung“ kontrovers diskutiert. Nach Auffassung des Bundesgerichtshofs ist gemäss geltendem Bundesrecht eine solche Massnahme für Zwecke der Strafverfolgung nicht zulässig. Er begründete seine Entscheidung u.a. damit, dass diese ohne Wissen der betroffenen Person stattfindet, während das Gesetz für eine herkömmliche Durchsuchung die Anwesenheit von ZeugInnen und des/r Inhabers/in des Durchsuchungsobjektes bzw. seines/r Vertreters/in vorsieht. Nach seiner Ansicht dürfen auch einzelne Elemente von Eingriffsermächtigungen nicht kombiniert werden, um eine Grundlage für eine neue technisch mögliche Ermittlungsmassnahme zu schaffen (BGH, Beschluss vom 31.1.2007 - StB 18/06).

Eine dem letzten Punkt entsprechende Bestimmung sieht auch die Schweizerische Strafprozessordnung in Art. 245 vor.

Für viele Menschen ist der Computer mit Internet-Anschluss zu einem zentralen Bestandteil der Lebensführung geworden. Das Deutsche Bundesverfassungsgericht hat daher in seinem Urteil zur „Online-Durchsuchung“ ein sich aus dem allgemeinen Persönlichkeitsrecht ergebendes „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ formuliert (BVerfG, 27.2.2008, Az. 1 BvR 370/07, 1 BvR 595/07).

Ein solches Grundrecht auf digitale Intimsphäre ergibt sich auch aus den Artikel 10, 7 und 13 der Schweizerischen Bundesverfassung.

Neben den rechtlichen stellen sich auch einige technische Fragen. Zunächst muss eine Möglichkeit gefunden werden, die Überwachungssoftware auf dem gewünschten Rechner zu installieren.

Das Ausnützen von bekannten Sicherheitslücken ist in der Praxis kaum möglich. Zu unterschiedlich sind die verwendeten Betriebssysteme, Versionen und Programme. Werden Lücken bekannt, sind die betroffenen Softwarehersteller und auch die Entwickler entsprechender Schutzsoftware (Firewalls, Antiviren-Programme etc.) darum bemüht, diese umgehend zu schliessen.

Um noch unbekannte Software-Lücken ausnutzen zu können (0day Exploits), müssten diese entweder selber gefunden oder für viel Geld eingekauft werden. Auch hier wäre der Aufwand pro Betriebssystem resp. sogar pro Betriebssystem-Version zu betreiben. Nutzbar bleibt eine solche Malware auch nur, bis die Lücke vom Hersteller geschlossen oder Abhilfe bekannt wird. In der Zwischenzeit könnte die Schadsoftware jedoch von der zu überwachenden Person an einen grösseren Personenkreis und möglicherweise sogar ins Ausland gelangen. Das Risiko einer solchen Verbreitung, durch Schweizer Behörden ausgelöst, kann nicht auf sich genommen werden.

Die Hersteller dazu zu verpflichten, sogenannte Backdoors für die Behörden einzubauen, ist nicht realistisch. Werden sie bekannt, sind sie durch spezialisierte Software problemlos zu schliessen. Oder schlimmer: auszunutzen. Es

ist auch kaum anzunehmen, dass ausländische Softwarehersteller für Schweizer Behörden entsprechende Lücken einbauen werden. Zudem gibt es neben MS-Windows und MacOS X unzählige weitere Betriebssysteme. Viele davon (Linux, *BSD etc.) werden nicht zentral entwickelt und stehen sogar im Quellcode zur Verfügung. Hier unbemerkt eine Hintertüre einzuschleusen, ist kaum denkbar.

Durch einen automatischen Download (Software-Updates) ein System zu infiltrieren, setzt genaueste Kenntnisse des Ziels voraus. Da heutzutage Updates in den allermeisten Fällen verschlüsselt und signiert vonstatten gehen, wäre auch hier eine Mitwirkung des Herstellers Voraussetzung. Wer wiederum auf offene Betriebssysteme und/oder auf signierte Updates setzt, kann die Überwachungsmassnahme umgehen.

Eine Möglichkeit wäre, die betroffene Person durch sogenanntes Social Engineering dazu zu verleiten, eine entsprechende Software selber zu installieren. Damit dies funktionieren kann, muss sowohl das Zielsystem wie auch die Zielperson genau gekannt werden. Unter Vorspiegelung falscher Tatsachen könnte dann der betroffenen Person die Überwachungssoftware per E-Mail-Anhang oder getarnt als offizielle Software der Behörden (beispielsweise als elektronische Steuererklärung) zugestellt werden. Es ist dabei nicht zu verhindern, dass die betroffene Person die Schadsoftware an Leute aus dem Freundes- und Bekanntenkreis weiterleitet oder auf einem Rechner am Arbeitsplatz installiert. Der Vorentwurf schweigt sich komplett darüber aus, wie dies gehandhabt werden soll. Entsprechende Regelungen und Schadensersatzpflichten sind nicht benannt. Im Falle einer getarnten Zustellung der Schadsoftware (beispielsweise als elektronische Steuererklärung) wird zudem der Ruf des vermeintlichen Absenders geschädigt.

Was bleibt, ist das heimliche Eindringen in die Räumlichkeiten und die Manipulation des Gerätes vor Ort. Ein solch schwerwiegender Eingriff in die Privatsphäre dürfte kaum mit dem Katalog der Anlassstraftaten, der aktuell sehr weit gefasst ist, zu rechtfertigen sein.

Selbst nach einer allfällig erfolgreichen und unbemerkten Installation bleiben weitere erhebliche technische Herausforderungen zu meistern.

Ein Zugang zum überwachten Gerät ist offensichtlich nur möglich, wenn dieses, wie auch die Internetverbindung, eingeschaltet ist. Um davon unabhängig eine Festplatte durchstöbern zu können, müssten die Daten kopiert werden. Handelsübliche Festplatten weisen heutzutage mehrere hundert Gigabyte Speicherplatz auf. Um z.B. 100 GB über einen Standard-DSL-Anschluss (max. Upload 500 kbit/s) zu übertragen, würden ca. 20 Tage benötigt.

Diese Aktionen dürften einer installierten Antiviren-Software oder Firewall nicht verborgen bleiben. Entsprechende Produkte verhindern mittlerweile nicht mehr nur die Ausführung bekannter Malware, sondern achten auch auf verdächtiges Verhalten: Falls ein Programm sich gegen eine Entdeckung zu

schützen sucht oder eine Verbindung „nach Hause“ aufnehmen will, schlagen sie Alarm. Es ist nicht anzunehmen, dass die Hersteller auf Wünsche Schweizer Behörden eingehen werden, eine Ausnahme in die Erkennungssoftware einzubauen. Dies würde ihrem ureigensten Geschäftsmodell zuwiderlaufen. Zumal eine entsprechende Lücke für den Trojaner Federal auch von einem anderen, „richtigen“ Schadprogramm - durch Imitation - ausgenutzt werden könnte.

Aus diesen Gründen kann es den „Trojaner Federal“ kaum als fertiges Software-Produkt geben. Um erfolgreich eingeschleust werden zu können, müsste er höchstwahrscheinlich massgeschneidert für die zu überwachende Person entwickelt und allenfalls mit der Hilfe von Drittpersonen installiert werden. Analoges gilt im Anschluss für den unbemerkten Betrieb. Die Wahrscheinlichkeit, die Software wiederverwenden zu können, ist gering - der Aufwand und die Kosten daher entsprechend gross. Zudem unterliegt der Zugang zum überwachten Objekt dessen technischen Einschränkungen (Bandbreite, Onlinezeiten etc.).

Der Gesetzesentwurf sieht zudem keine Pflicht für eine Deinstallation des „Trojaner Federal“ nach Abschluss der Ermittlungen vor.

Trotz des schwerwiegenden Eingriffs in die Privatsphäre, können Zufallsfunde verwendet werden (StPO Art. 278).

Auch eine Mitteilung an die betreffende Person nach Abschluss der Überwachung ist nicht zwingend, wenn „die Erkenntnisse nicht zu Beweiszwecken verwendet werden; und der Aufschub oder das Unterlassen zum Schutze überwiegender öffentlicher oder privater Interessen notwendig ist“ (StPO Art. 279.2). Um die beteiligten Provider und Anbieter zu schützen und das angewandte Verfahren geheim zu halten, dürfte in der Regel wohl auf eine Benachrichtigung verzichtet werden (es sei denn, die Zwangsmassnahme ist ohnehin schon bekannt geworden).

Als weiteres Risiko gilt zudem zu erwähnen, dass die von der Überwachung betroffene Person einen Gegenangriff starten könnte: Technisch versierte BenutzerInnen werden einen „Trojaner Federal“ auf ihrem System bemerken. Durch eine Analyse kann dann festgestellt werden, welche Daten, in welchem Format und wohin übertragen werden. Dadurch wird es möglich, die übertragenen Informationen zu fälschen oder es kann versucht werden, das Empfangssystem durch präparierte Daten zum Absturz zu bringen oder einen Datenverlust zu provozieren.

Die Swiss Privacy Foundation fordert, auf eine rechtsstaatlich bedenkliche, technisch schwierige und im Einzelfall teure „Online-Durchsuchung“ zu verzichten.

7 IMSI-Catcher (Ortungsgeräte)

Gemäss vorliegendem Entwurf soll mit Artikel 270ter StPO der Einsatz von Ortungsgeräten angeordnet werden können. Damit sind laut erläuterndem Bericht speziell sogenannte IMSI-Catcher gemeint (Seite 44 Abs. 4).

Diese Geräte verhalten sich im Mobilfunknetz gegenüber einer Basis-Station wie ein Handy und gegenüber einem Handy wie eine Basis-Station. Sobald das Signal des IMSI-Catchers gegenüber den Handys im Empfangsbereich stärker ist, wie das der ursprünglichen Basis-Station, buchen sich diese automatisch neu via Catcher in das Mobilfunknetz ein. Da sich eine Basis-Station nicht gegenüber einem Handy authentisieren muss, diese jedoch darüber bestimmen kann, ob eine Verschlüsselung eingesetzt wird oder nicht, kann der IMSI-Catcher nun als Man-In-The-Middle die Kommunikation sämtlicher Geräte im Empfangsbereich mitschneiden.

Damit Verbindungen ins Telefonnetz möglich bleiben, meldet sich der IMSI-Catcher selber bei der nächstgelegenen regulären Basis-Station an. Da er sich dabei jedoch nur als ein Mobiltelefon (mit einer einzigen, unterdrückten Rufnummer) ausgeben kann, sind für alle bei ihm eigebuchten Handys nur abgehende aber keine ankommenden Verbindungen möglich. Korrekt hält der erläuternde Bericht dann auch fest, dass die „erwähnten Geräte [..., geeignet sind] den Fernmeldeverkehr zu stören“ (Seite 44 Abs. 6). Jedoch ändert sich daran auch nichts, wenn sie von den zuständigen Behörden - wie vorgesehen - bewilligt worden sind.

Falls ein zu überwachendes Handy bekannt ist, kann dieses herkömmlich via Mobilfunkanbieterin überwacht werden. Der IMSI-Catcher kommt also zum Tragen, wenn ein ungefährer Ort, nicht jedoch der Anschluss bestimmbar ist. Da sich sämtliche Handys im Empfangsbereich (ob gewollt oder nicht) zum IMSI-Catcher verbinden, sind auch Unbeteiligte von der Massnahme betroffen, ohne dass sie davon erfahren.

Da ein IMSI-Catcher den Mobilfunk erheblich beeinträchtigt und in grossem Masse Unbeteiligte von der Überwachung betroffen sind, fordert die Swiss Privacy Foundation, den Einsatz solcher Geräte zu verbieten.

8 Vorratsdatenspeicherung

In Artikel 19 bzw. 23 des Vorentwurfs wird die Aufbewahrungspflicht für Randdaten im Post- und Fernmeldeverkehr von den im geltenden Recht geregelten 6 Monaten auf 12 Monate erhöht. Aus diesem, aber auch aus anderen, nachfolgend noch darzulegenden Gründen, ist die im Vorentwurf vorgesehene Regelung der Datenaufbewahrung aus Sicht der Swiss Privacy Foundation nicht haltbar.

Der Brief-, Post- und Fernmeldeverkehr ist durch Artikel 13 der Bundesverfassung als Grundrecht geschützt. Jede Kenntnisnahme, Aufzeichnung und Verwertung von im Rahmen des Brief,- Post- und Fernmeldeverkehrs entstehenden Daten durch die öffentliche Gewalt stellt daher grundsätzlich eine Verletzung dieses Grundrechts dar, welche nur unter strengen Voraussetzungen zulässig ist. Je schwerwiegender der Eingriff in das Grundrecht ist, umso höhere Anforderungen sind an dessen Zulässigkeit zu stellen.

Die verdachtsunabhängige Speicherung von Verbindungs-, Verkehrs- und Rechnungsdaten stellt zweifelsohne einen erheblichen Eingriff in das Brief-, Post- und Fernmeldegeheimnis dar: Zunächst ist zu berücksichtigen, dass die Erhebung dieser sogenannten „Randdaten“ für die gesamte Bevölkerung und zunächst ohne jeglichen Anlass erfolgt. Betroffen von der Massnahme sind ausnahmslos alle, wobei bezogen auf den Grossteil der Bevölkerung nur ein hypothetisches Interesse an den Daten (zur Verfolgung von schweren Straftaten) besteht. Es geht hier also 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- (Festnetz, Mobiltelefonie, Fax, SMS, MMS etc.), E-Mail- und Internetdiensten - mit der Absicht, die Daten bei Bedarf gezielt auswerten zu können.

Zu berücksichtigen ist auch, dass sich das Kommunikationsverhalten in den letzten Jahren massiv verändert hat. Durch die Vielfältigkeit der Kommunikationsmittel und die Häufigkeit der Benutzung bilden die zu erhebenden Verbindungsdaten das Kommunikationsverhalten der Bevölkerung praktisch vollständig ab. Nahezu jede Kontaktaufnahme wird aufgezeichnet, inklusive des genauen Zeitpunkts und teils sogar des Standorts. Die Auswertung dieser umfangreichen Daten ermöglicht daher tief in das Privatleben eingreifende Rückschlüsse über soziale Kontakte und die Anfertigung detaillierter Persönlichkeits- und Bewegungsprofile, so dass auch gewisse Rückschlüsse über den Inhalt der Kommunikation möglich sind.

Die Massnahme ist geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann. Unterschiedslos sind davon auch die Hilfesuchenden und MitarbeiterInnen von Organisationen betroffen, die auf Vertraulichkeit angewiesen sind und anonyme Beratung in seelischen oder sozialen Notlagen anbieten.

Aufgrund der soeben dargelegten Schwere des Eingriffs in das Brief-, Post- und Fernmeldegeheimnis sind die Anforderungen für dessen Rechtfertigung hoch anzusetzen. Diesen genügt der Entwurf - wie auch die Regelung im geltende Recht - nach Ansicht der Swiss Privacy Foundation nicht.

Die das Grundrecht einschränkende Gesetzesbestimmung muss gemäss Bundesgericht „so präzise formuliert sein, dass der Bürger sein Verhalten danach richten und die Folgen eines bestimmten Verhaltens mit einem den Um-

ständen entsprechenden Grad an Gewissheit erkennen kann“ (BGE 117 Ia 472, S. 480). Durch dieses Erfordernis werden sowohl die Rechtssicherheit als auch die Rechtsgleichheit gewährleistet (Häfelin/Haller, a.a.O., Rz. 308 f.). Gemäss Bundesverfassung müssen zudem schwerwiegende Eingriffe im Gesetz selbst und nicht etwa in einer Verordnung geregelt sein (Art. 36 Abs. 1).

Diesen Erfordernissen genügen sowohl die geltenden Artikel 12 Abschnitt 2 und 15 Abschnitt 3 BÜPF als auch die Artikel 19 Abschnitt 2 bzw. 23 aus dem Vorentwurf nicht. Letztgenannter enthält zwar im Vergleich zu Artikel 15 Abschnitt 3 des geltenden BÜPF bereits eine viel konkretere Umschreibung der zu erhebenden Daten (was die Swiss Privacy Foundation sehr begrüsst), erwähnt aber beispielsweise überhaupt nicht die Erfassung des Antennenstandorts bei Mobilfunkverbindungen, welche heute in der Verordnung zum BÜPF (Art. 16 lit. d Ziff. 3) vorgeschrieben ist. Soweit eine solche Standorterfassung auch in Zukunft vorgesehen ist, gilt es, sie auf Gesetzesstufe zu regeln. Insbesondere die wagen Begriffe „Anschlüsse“, „Verbindungen“ und „Verkehrsdaten“ sind auf dieser Ebene genauer zu umschreiben.

Eine weitere Voraussetzung für einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis ist dessen Verhältnismässigkeit. Verhältnismässig ist ein Eingriff dann, wenn er überhaupt für das Erreichen des angestrebten Zwecks geeignet ist, das Ziel nicht mit einer weniger invasiven Massnahme erreicht werden kann und das Verhältnis zwischen Eingriffszweck und Eingriffswirkung in einem vernünftigen Rahmen bleibt.

Dass die Aufbewahrung von Daten auf Vorrat grundsätzlich geeignet sein kann, die Verfolgung von schweren Straftaten zu erleichtern, wird von der Swiss Privacy Foundation im Grundsatz nicht in Abrede gestellt. Trotzdem müssen diesbezüglich vor allem im Bereich Internet erhebliche Zweifel angebracht werden, ist es doch für versierte Benutzer ein Leichtes, die Aufzeichnung des E-Mail-Verkehrs, der Internettelefonie etc. durch Verschlüsselung, Nutzung von Proxy-Servern, Verwendung von Diensten im Ausland o.Ä. zu umgehen. Es ist somit höchst unklar, ob die Datenaufbewahrung im Bereich organisierte Kriminalität, mit dem sie überhaupt erst legitimiert wird, zur Erreichung des Zwecks geeignet ist.

Auch bezüglich der Erforderlichkeit des Eingriffs sind erhebliche Vorbehalte anzubringen: Bereits die Speicherungsdauer von 6 Monaten erscheint aufgrund der oben dargelegten Schwere des Eingriffs nicht gerechtfertigt. So hat das Deutsche Bundesverfassungsgericht denn auch, als es in Deutschland darum ging, die Verfassungsmässigkeit der dortigen Vorratsdatenspeicherung zu überprüfen, im Urteil vom 2. März 2010 festgehalten, dass „eine Speicherungsdauer von sechs Monaten angesichts des Umfangs und der Aussagekraft der gespeicherten Daten sehr lang sei und an der Grenze dessen läge, was unter Verhältnismässigkeitserwägungen rechtfertigungsfähig sei“. Ebenso erscheint die Speicherung von Standortdaten im Mobilfunkbereich nicht notwendig, da der Zweck der Datenaufbewahrung, nämlich das Erkennen von kriminellen Netz-

werken, insbesondere im Bereich Kinderpornographie, organisiertes Verbrechen und Betäubungsmittel, bereits durch die übrigen Verbindungsdaten weitgehend gewährleistet ist. Der Mehrwert der Daten, der durch die zusätzliche Erfassung des Standorts generiert wird, erscheint - sofern er überhaupt gegeben ist - im Verhältnis zum einhergehenden Eingriff in die Privatsphäre, der das Erstellen eines Bewegungsprofils über fast jeden/e BürgerIn ermöglicht, von wesentlich geringerem Gewicht.

Die Verlängerung der Aufbewahrungsfrist ist, wie dem erläuternden Bericht zu entnehmen ist, auf die teilweise Annahme der Motion 06.3170 von Rolf Schweiger zurückzuführen. Diese bezieht sich jedoch einzig auf die Aufbewahrungsdauer für Internetanbieter. In erwähnter Motion wird ausgeführt: „Die praktische Erfahrung hat gezeigt, dass die Aufbewahrungspflicht für Logbuchdateien seitens der Internetanbieter zeitlich zu knapp bemessen ist und den Strafverfolgungsbehörden für ihre Nachforschungen oft schlicht die Zeit fehlt."

Die Verlängerung der Aufbewahrungsfrist auf 12 Monate, wie sie vorgesehen ist, verdient in diesem Zusammenhang zweifache Kritik:

- Erstens können mangelnde Ressourcen bei den Strafverfolgungsbehörden keine Rechtfertigung für einen derart schwerwiegenden Eingriff in die Grundrechte der gesamten Wohnbevölkerung der Schweiz sein! Die Erhöhung ist schlicht nicht erforderlich, da der Zweck auch mit anderen Massnahmen erreicht werden kann, die weniger stark in die Privatsphäre jedes/r einzelnen Bürgers/in eingreifen. Untersuchungen in der EU (Evaluation of Directive 2006/24/EC) haben überdies ergeben, dass die Relevanz der Daten mit ihrem Alter erheblich sinken. Demnach würden sich 70 Prozent der Abfragen der Verbindungs- und Standortinformationen auf maximal drei Monate beziehen. Entsprechende Statistiken für die Schweiz fehlen leider - auch im erläuternden Bericht.

- Zweitens erscheint die Erhöhung, selbst wenn die Erforderlichkeit in Bezug auf das Internet bejaht würde, zumindest im Bereich des Brief-, Post- und und Fernmeldeverkehrs, in keiner Weise gerechtfertigt, da es hier erst recht an der Erforderlichkeit der Massnahme fehlt. Es ist erstaunlich, mit welcher Leichtfertigkeit im Entwurf eine massive Verschärfung eines Grundrechtseingriffs vorgesehen wird, wo ein solcher weder gefordert, geschweige denn erforderlich ist. Zudem ist zu bemerken, dass die teilweise Annahme der Motion 06.3170 von Rolf Schweiger nicht die geforderte Ausdehnung der Aufbewahrungspflicht von 6 auf 12 Monaten beinhaltet.

Das Deutsche Bundesverfassungsgericht hat mit bereits oben erwähntem Urteil - auf eine von 34'000 BürgerInnen getragene Beschwerde hin - die praktizierte Vorratsdatenspeicherung nicht nur für unvereinbar mit dem Grundgesetz erklärt, sondern auch die unverzügliche Löschung der bis anhin gesammelten

Daten angeordnet. Dies im Gegensatz zur Behauptung aus dem erläuternden Bericht, wonach das deutsche Recht vorsehen würde, „dass diejenigen Daten, die unseren sogenannten Randtaten (sic!) entsprechen, von den Anbietern von Fernmeldedienstleistungen während sechs Monaten aufbewahrt werden müssen“ (Seite 14 Abs. 4).

Sämtliche Verfassungsgerichte (Deutschland, Irland, Bulgarien und Rumänien), welche die nationale Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung zu beurteilen hatten, haben sie als nicht verfassungsmässig eingestuft. Auch die schwedische Regierung weigert sich, ein entsprechendes Gesetz zu erlassen. 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.

Mit den umfassenden Informationen aus der Vorratsdatenspeicherung lassen sich präzise Persönlichkeitsprofile erstellen. Diese dürften auch für die aufzeichnenden Firmen von Interesse sein. Im Vorentwurf sind weder entsprechende Regelungen zur Datensicherheit noch Sanktionen bei unrechtmässiger Verwendung der Informationen vorgesehen. Es wird ebenfalls darauf verzichtet, die Löschung der Daten nach Ablauf der Aufbewahrungsfrist vorzuschreiben.

Gemäss erläuterndem Bericht (Seite 17 Abs. 3 und 4) sind Internetcafés, Schulen, Hotels, Restaurants, Spitäler etc., die beispielsweise ihren KundInnen Wi-Fi zur Verfügung stellen, keine Internetanbieterinnen, die ihre Tätigkeit - nach dem Gesetz - berufsmässig ausüben: Sie sind also nicht zur Überwachung verpflichtet, jedoch angehalten, entsprechende Massnahmen zu dulden (Vorentwurf Art. 2). Demnach dürfte für sie auch Artikel 22 nicht gelten. Doch in diesem Fall unterstellt sie der erläuternde Bericht der Identifizierungspflicht (Seite 33 Abs. 3). Das Beispiel zeigt, dass auch den AutorInnen nicht klar ist, was mit „berufsmässig ausüben“ gemeint ist. Muss der Firmenzweck das Anbieten einer Internetdienstleistung beinhalten, um vom Artikel erfasst zu werden, oder reicht es schon, diese im Rahmen einer Berufstätigkeit (also nebenbei) auszuüben?

Dies ändert jedoch nichts an der Tatsache, dass der Geltungsbereich des BÜPF gemäss Vorentwurf neu nicht mehr „nur“ auf Access Provider, sondern zusätzlich auch auf Hosting-, Housing- und Contentprovider erweitert werden soll. Für die professionellen Anbieterinnen würde demnach ebenfalls die verdachtsunabhängige und flächendeckende Vorratsdatenspeicherung gelten. Der entsprechende Artikel 23 aus dem Vorentwurf ist jedoch auch dahingehend ungenau: Sie sind nämlich verpflichtet darüber Auskunft zu geben, „wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindungen hat oder gehabt hat [...] während zwölf Monaten aufzubewahren“. Im Falle der Access Provider bedeutet dies sicherlich (wie bis anhin), dass IP-Zuordnungen und E-Mail-Verbindungen festgehalten werden müssen. Ist ein Webserverbetreiber nun aber angehalten, sein Serverlog mit den (IP-)Verbin-

dungsdaten aufzubewahren? Gilt dies grundsätzlich für sämtliche Serverbetreiber und Diensteanbieter? Muss neu ein Logfile geführt werden, wenn bis anhin keine solchen personenbezogenen Daten aufgezeichnet worden sind? Und bedeutet dies für den Access Provider sogar, dass alle IP-Verbindungen - und somit ein komplettes Online-Bewegungsprofil - sämtlicher NutzerInnen vorgehalten werden müssen? Oder kann im Bereich E-Mail (und anderen Diensten) gar nicht von „Anschlüssen“ gesprochen werden? Von einer präzisen Formulierung, die für Rechtssicherheit sorgt, ist der Entwurf auch hier weit entfernt!

Ein Provider macht sich strafbar, wenn er diese personenbezogenen und grundgesetzlich geschützten Daten ohne rechtliche Grundlage bearbeitet. Er kann aber gemäss Vorentwurf ebenfalls mit bis zu 100'000 Franken (Art. 31) gebüsst werden, falls er der Datenaufbewahrung nicht nachkommt. Dieser dünne Grat muss klar definiert sein. Eine präzise Umschreibung des Geltungsbereichs und des Gegenstandes auf Gesetzesstufe ist daher unabdingbar.

Ebenfalls ungenügend sind die Bestimmungen zum Postverkehr. Bis anhin sind sie nur ungenau. Immerhin spricht das Gesetz in Artikel 12 lediglich von einer Aufbewahrungs- und nicht von einer Erhebungspflicht und die Verordnung von „sämtlichen verfügbaren Daten“ (Art. 12 lit. c Punkt 2). Neu heisst es im Vorentwurf in Artikel 19 jedoch: „Wann und mit welchen Personen die überwachte Person über den Postverkehr Verbindungen hat oder gehabt hat, sowie Verkehrs- und Rechnungsdaten [...] während zwölf Monaten aufbewahren.“

Das würde nichts Geringeres bedeuten, als dass die Post (an jedem Briefkasten) die Identität von sämtlichen Personen feststellen müsste, die einen Brief versenden möchten und auch die Empfängeradressen für 12 Monate vorzuhalten hat. Immerhin kann dem Vorentwurf nicht mangelnde Konsequenz vorgeworfen werden: Denn damit wird für den Postverkehr nichts anderes gefordert, als was für E-Mails bereits mit aktuellem Recht gilt.

Zusammenfassend:

- Der Brief-, Post- und Fernmeldeverkehr ist nach Bundesverfassung Art. 13 geschützt. Schwere Eingriffe in dieses Grundrecht müssen hohen Anforderungen genügen, welche durch diesen Vorentwurf nicht gegeben sind.
- Die „rückwirkende Überwachung“ ist eine flächendeckende und verdachtsunabhängige Überwachung, von welcher alle EinwohnerInnen der Schweiz betroffen sind - und daher nicht verhältnissmässig.
- Die 12 monatige Speicherung der Randdaten ermöglicht es, ein detailliertes Kommunikations- und Bewegungsprofil sämtlicher BürgerInnen der Schweiz zu erstellen.
- Die Notwendigkeit der Verdoppelung der Speicherungsdauer ist nicht nachgewiesen. Im Gegenteil: Studien in der EU haben gezeigt, dass alte Daten nicht mehr relevant sind.

- Das Deutsche Bundesverfassungsgericht hat die praktizierte Vorratsdatenspeicherung für unvereinbar mit dem Grundgesetz erklärt. Analog haben auch andere Verfassungsgerichte in Europa entschieden.
- Die Ausdehnung der Erfassungspflicht auf Randdaten im Postverkehr ist unbegründet.
- Die formulierte Ausdehnung der Erfassungspflicht auf Randdaten bei Hosting-, Housing- und Contentprovider, ebenso bei Mobilfunkanbietern, ist zu vage.
- Die Überwachungsarten, die zu speichernden Daten und die verwendeten Begriffe sind im Vorentwurf nicht genügend definiert.

Die Swiss Privacy Foundation lehnt eine anlassunabhängige Vorratsdatenspeicherung ab. Falls auf diese rechtsstaatlich bedenkliche Massnahme nicht verzichtet werden kann, muss sie unter strengsten Auflagen vorgenommen werden. Die Personen und Daten, welche vom Gesetz betroffen sind, müssen genau bezeichnet und auf möglichst wenige beschränkt sein. Die Aufbewahrungsfrist darf nicht auf 12 Monate verlängert werden.

9 Schlussbetrachtung

Der vorgelegte Entwurf schiesst weit über das Ziel hinaus. Er liest sich streckenweise wie ein Wunschzettel einer Überwachungsbehörde und erweitert entgegen den Beteuerungen aus dem erläuternden Bericht den Gegenstand des BÜPF beträchtlich:

- Aktive Überwachungspflicht für sämtliche professionellen Anbieterinnen von Dienstleistungen und Inhalten im und zum Internet
- Passive Mitwirkungspflicht für alle nicht professionellen Anbieterinnen und Privatpersonen
- Ausdehnung der Überwachung von E-Mail, Telefon und SMS auf den kompletten Datenverkehr
- Entzug der Rekursmöglichkeiten der Provider
- Erweiterung des Straftatenkatalogs, zu deren Verfolgung eine Überwachung angeordnet werden kann
- Zertifizierungszwang und Streichung der Entschädigung für die Provider
- Verdecktes Eindringen, Durchsuchung und Anbringen von Schad-/Überwachungssoftware in fremden Computern

- Einsatz von IMSI-Catchern
- Verdoppelung der Speicherdauer betreffend der gewonnenen Daten aus der flächendeckenden und verdachtsunabhängigen Überwachung der NutzerInnen von Telefon-, E-Mail- und Internetdiensten

Diesen Forderungen entgegen steht der verfassungsmässig garantierte Schutz der Privatsphäre und die Verhältnismässigkeit hinsichtlich des technischen und finanziellen Aufwands. Diesen Aspekten wird in der aktuellen Revision nicht angemessen Rechnung getragen.

Die Nützlichkeit der neu geplanten oder erweiterten Massnahmen lässt sich zudem zum aktuellen Zeitpunkt kaum bewerten. Im Vorentwurf werden keine Statistiken über die bisher durchgeführten Überwachungen angeführt, aus denen ersichtlich wäre, welchen Nutzen diese haben - und wo Handlungsbedarf besteht. Eine Ausweitung in vorliegendem Umfang ins Blaue zu planen, ist nicht akzeptabel.

Aus den dargelegten Gründen lehnt die Swiss Privacy Foundation den vorgelegten Revisionsentwurf ab. Der Verein anerkennt gewisse Mängel am gültigen Gesetz und fordert daher, die Revision grundsätzlich und gründlich zu überarbeiten:

- Eine genauere Definition des Geltungsbereichs ist wünschenswert. Das Gesetz hat jedoch im Bereich Internetüberwachung weiterhin nur für professionelle Access Provider zu gelten.
- Die Definition der Datenarten, welche im Rahmen einer Überwachung angeordnet werden können, müssen auf Gesetzesstufe geregelt werden. Sie sind als „E-Mail“, „Telefongespräche (auch über das Internet)“, „Textnachrichten (wie SMS)“ etc. festzuhalten - und dürfen nicht pauschal „den gesamten Datenfluss“ betreffen.
- Es ist per Gesetz die Möglichkeit vorzusehen, dass ein betroffener Provider die Rechtmässigkeit einer Überwachungsanordnung gerichtlich überprüfen lassen kann.
- Die Kosten für die Überwachung ist den Providern zu entschädigen. Auf eine Zertifizierung ist zu verzichten.
- Die Erweiterung des Katalogs der Anlassstraftaten ist kritisch zu hinterfragen. Er hat zudem auch für den Zugriff auf Daten aus der Vorratsdatenspeicherung („Rückwirkende Überwachung“, Identifizierungspflicht) zu gelten.
- Auf die Möglichkeit einer „Online-Durchsuchung“ ist zu verzichten.
- Der Einsatz von IMSI-Catchern ist zu verbieten.

- Eine verdachtsunabhängige und flächendeckende Vorratsdatenspeicherung hat in einem freiheitlichen Rechtsstaat nichts verloren. Falls auf diese Massnahme nicht verzichtet werden kann, darf sie nur unter strengsten Auflagen vorgenommen werden. Die Aufbewahrungsfrist der Daten darf nicht auf 12 Monate verlängert werden.