



EINGESCHRIEBEN

Bundesamt für Justiz
Direktionsbereich Strafrecht
Bundesrain 20
3003 Bern

Zürich, 17. August 2010

Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung von Post- und Fernmeldeverkehr – Vernehmlassungsantwort

Sehr geehrte Damen und Herren

Wir gestatten uns, Ihnen in der Beilage unsere Stellungnahme zur Totalrevision des Bundesgesetzes zur Überwachung von Post- und Fernmeldeverkehr (BÜPF) zukommen zu lassen. Obschon wir nicht auf der Liste der von Ihnen dazu eingeladenen Personen figurieren, erachten wir es als unsere Pflicht und Aufgabe, Ihnen unser Haltung zu den einzelnen, unsere Branche betreffenden Artikel zu kommen zu lassen. Wir danken Ihnen, wenn Sie diese bei der Auswertung der Vernehmlassungsergebnisse gebührend berücksichtigen.

Die von Ihnen formulierte Zielsetzung, wonach die Überwachungsinstrumente dem technischen Fortschritt entsprechen müssten, begrüssen wir. Allerdings sind aus unserer Sicht einige Verbesserungen nötig, damit die im Bereiche tätigen Unternehmer ihre Tätigkeit auch inskünftig in guten Rahmenbedingungen ausüben können.

Es ist unbestritten, dass die modernen Formen der Cyber-Kriminalität nach einer **Erweiterung der Untersuchungsmittel** der Strafverfolgungsbehörden rufen. Die wesentlich erweiterten Verfahren zur Erfassung der Identität der Kommunikationspartner im Internet, die zusammenfassende langfristige Speicherung aller Daten aus der elektronischen Überwachung in einem grossen zentralen System (mit den dadurch geschaffenen Auswertungsmöglichkeiten), Identifizierung sämtlicher Benützer des Internet; der vorgesehene Einsatz von "Bundes-Trojanern", ruft jedoch nach entsprechenden Kontrollvorkehrungen: Nicht nur die Spiesse der Strafverfolgungsbehörden und der Cyber-Kriminellen sollten gleich lang sein, sondern auch die Spiesse der Behörde und der in ihrer Privatsphäre und ihrer grundrechtlich geschützten Kommunikation betroffenen Bürger.

Seite 2/7

Dies zumal die im RevE BÜPF vorgesehene Übertragung der organisatorisch-technischen Überwachungsmassnahmen und der damit verbundenen **zusätzlichen Aufgaben** für die Fernmeldediensteanbieter und ISP, wie z.B. die neu geschaffene Zertifizierungspflicht, die Qualitätskontrolle, die Verdoppelung der Aufbewahrungsdauer der Randdaten, die Identifizierung aller Internet-Benutzer an öffentlichen zugänglichen Orten wie Hotels, Schulen, Restaurants, die Entfernung von privaten Schlüsseln, die Triage der bei der Überwachung erfassten Daten usw. eine nicht unerhebliche zusätzliche Belastung der Privatwirtschaft nach sich zieht.

Kritisch beurteilen wir zudem die Frage der **Kosten**. Überwachungen im technologischen Bereich sind in Anschaffung und Betrieb sehr kostspielig. Eine gute Balance zwischen Kosten und Nutzen ist sichergestellt, wenn die behördlichen Überwachungsmassnahmen einheitlich und nicht kantonale unterschiedlich sind. Muss die Behörde die Kosten ihrer Untersuchung nicht mehr tragen, dann drohen die Kosten aus dem Ufer zu laufen. Die Kosten müssten dann die Wirtschaft und die Konsumenten tragen. Dies wäre sicher nicht richtig und es ist aus unserer Sicht unakzeptabel.

Ebenso sollten künftig klare **Rechtsmittel** bestehen für den Fall überbordender behördlicher Ansprüche. Dies ist bis heute nicht vorgesehen und wir vermissen entsprechende Vorschriften auch im total revidierten vorliegenden Gesetz.

Wir gestatten uns, Ihnen zu den einschlägigen Gesetzesartikeln entsprechende Änderungsvorschläge zu unterbreiten:

Art. 6 Grundsatz

Der Dienst betreibt ein Informatiksystem zur Verarbeitung der durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten.

Wir begrüssen die Bestimmung im Art. 33, wonach der zentrale Dienst über die Einhaltung der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs wacht.

Diese Bestimmung ist allerdings im vorgelagerten Artikel 6 zu ergänzen: Mit klaren Vorschriften über die nötigen Kontrollen des grossen zentralen Speichers aller Überwachungsdaten sowie mit einer klar strukturierten Definition der Aufgaben des zentralen Dienstes.

Art. 11 Aufbewahrungsfrist von Daten

Die Daten über den Fernmeldeverkehr der überwachten Personen sollen zwischen 5 und 30 Jahren aufbewahrt werden können.

Seite 3/7

Art. 11. ist mit Bestimmungen zu ergänzen, wer (welche Instanz) über die tatsächliche Dauer der Aufbewahrung im jeweiligen Fall bestimmt. Ebenfalls ist zu bestimmen, wer über eine allfällige Vernichtung der Daten entscheidet.

Art. 18/24 Zertifizierung

Zertifizierung der Anbieter von Fernmeldediensten auf deren eigenen Kosten durch den zentralen Dienst.

Gegenstand und Verfahren der Zertifizierung sind zu präzisieren und genauer zu umschreiben. Ferner muss Art. 18 klar machen (Aufzählung, Definition), wer genau sich zertifizieren lassen muss.

Art. 20 Auskünfte über Fernmeldeanschlüsse

⁴ Der Bundesrat regelt die Form der Gesuche und deren Aufbewahrung. Er kann den Behörden nach Artikel 14 den Zugriff auf bestehende nicht öffentliche Verzeichnisse gestatten. Er kann auch diese Daten dem Dienst durch ein Abrufverfahren zugänglich machen. Er kann vorsehen, dass die Mitteilung kostenlos und rund um die Uhr zu erfolgen hat.

Der in Artikel 20 vorgeschriebene Zugriff auf sämtliche Kommunikationsdaten und die somit sicher gestellte Identifikation der Teilnehmenden sichert den Bundesbehörden umfassende Überwachungsmöglichkeiten zu.

Im Sinne der beabsichtigten besseren, aber nicht umfassenderen Überwachung erklären wir uns mit diesem Artikel im Grundsatz einverstanden. Allerdings fordern wir, dass im Artikel 20 (bspw. als ein Art. 20 / 5 eine externe Kontrollinstanz benannt und definiert wird, welche den zentralen Dienst zu jedem Zeitpunkt überwacht und kontrolliert. Die umfassende Definition einer externen Kontrolle hat möglichst detailliert nicht nur im Gesetz sondern auch anschliessend in der Verordnung zum Gesetz zu geschehen.

Art. 21 Pflichten bei der Durchführung von Überwachungen

¹ Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, müssen dem Dienst auf Verlangen den Fernmeldeverkehr über den Anschluss der überwachten Person, welcher von der verpflichteten Anbieterin zur Verfügung gestellt wird, zuleiten.

² Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, liefern die Daten, welche darüber Auskunft geben, wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie Verkehrs- und Rechnungsdaten so rasch als möglich und den Fernmeldeverkehr der überwachten Person soweit möglich in Echtzeit. Von ihnen angebrachte Verschlüsselungen müssen sie entfernen.

Wir lehnen Art. 21 in dieser Form ab und fordern folgende Anpassungen:

1.

Da sich die Entschlüsselung auch auf die offen zu legenden Telekommunikationsdaten nach Art. 14 und 20 bezieht, ist festzuschreiben, dass die Fernmeldediensteanbieter und die ISP ihre vom zentralen Dienst zur Überwachung identifizierte Kunden noch vor der Einleitung des Überwachungsverfahrens darüber zu unterrichten haben, dass die verwendete Verschlüsselung im Rahmen eines Überwachungsverfahrens nach BÜPF aufgehoben werden und der Kunde in Folge dessen Gegenstand der Überwachung wird.

2.

Wir schlagen folgende Formulierung vor: „Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, liefern die Daten, welche darüber Auskunft geben, wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie Verkehrs- und Rechnungsdaten und den Fernmeldeverkehr der überwachten Personen. Von ihnen angebrachte Verschlüsselungen müssen sie entfernen.“

Die im Vorentwurf enthaltene Forderung, die Daten seien „so rasch als möglich“ und „soweit als möglich in Echtzeit“ zu liefern, ist unpräzise und in der Sache inakzeptabel. Dies zumal sie auch rein formal in der technischen Umsetzung äusserst fragwürdig wäre.

Grundsätzlich käme eine Daten-Lieferung in Echtzeit einem direkten Zugriff der Behörden auf die Daten von Kunden gleich. Dies würde also erfolgen, ohne dass der Fernmeldediensteanbieter und die ISP in der Lage wären, die Betroffenen über die Überwachung vorgängig zu informieren.

Auf eine „Echtzeit“- Forderung ist deshalb aus grundsätzlichen Überlegungen und auch was die Verhältnismässigkeit in der technischen Umsetzbarkeit angeht, zwingend zu verzichten.

3.

Die im Artikel 21 umschriebene, detaillierte und umfassende Überwachung des gesamten Datenflusses kommt einer Offenlegung des gesamten Datenverkehrs und somit einer vollständigen Überwachung einer Person gleich – analog einer eigentlichen Hausdurchsuchung. Wir fordern deshalb, dass eine solche Überwachung ausschliesslich auf richterlichen Entscheidung erfolgen darf. Dieser ist den Fernmeldediensteanbietern und den ISP vorgängig vorzulegen.

Art. 21 ist mit einer entsprechenden Bestimmung zu ergänzen.

³ Die Aussonderung von bestimmten Typen von Daten aus dem Datenstrom kann nur verlangt werden, insoweit dies mit den bei den Anbieterinnen von Fernmeldediensten installierten Anlagen möglich ist. Die Anbieterinnen von Fernmeldediensten sind jedoch verpflichtet, Überwachungsanlagen nach den international gängigen Normen zu betreiben.

Der mit dieser möglichen Triage verbundene hohe Aufwand ist von der Behörde zusätzlich zu entschädigen. (vgl. auch Art. 30).

Es müssen Rechtsmittel gegen Anordnungen geschaffen werden, die über die Pflichten hinausgehen. Auf diesem Weg wird eine Vereinheitlichung und Rechtsicherheit ermöglicht. Hingegen darf die Kompetenz der Ermittlungsbehörden bei der Anordnung von Überwachungen nicht durch die Fernmeldediensteanbieter in Frage gestellt sein. Wir bitten Sie, Art. 15 a) sowie Art. 34 entsprechend anzupassen:

Art. 15 Allgemeine Aufgaben der Überwachung

Er prüft, ob die Überwachung von einer zuständigen Behörde angeordnet wurde, ob die Art der angeordneten Überwachungsmaßnahme gesetzlich vorgesehen ist und ob die Art der angeordneten Überwachungsmaßnahme in technischer und organisatorischer Hinsicht durchgeführt werden kann. Er prüft nicht, ob die Anordnung einer Überwachung im konkreten Einzelfall die Voraussetzungen gemäss Art. 269 lit. b. und c. der Strafprozessordnung erfüllt und ob die Anordnung angemessen ist.

Art. 34 Rechtsschutz

¹ Verfügungen des Dienstes unterliegen der Beschwerde nach den allgemeinen Bestimmungen über die Bundesrechtspflege.

² Mit der Beschwerde gegen die Verfügung des Dienstes kann nicht geltend gemacht werden, die Anordnung einer Überwachung sei im konkreten Einzelfall unverhältnismässig oder die anordnende Behörde habe ihr Ermessen unrichtig ausgeübt.

ff Art 21

⁴ Fernmeldediensteanbieterinnen und ISP sind verpflichtet, dem zentralen Dienst bei der Überwachung zu unterstützen, für welche Informatikprogramme nach Art. 270^{bis} StPO zum Abfangen und Lesen von Daten erforderlich sind.

Laut Art. 270 bis StGB können auch Spionageprogramme („Bundes-Trojaner“) zum Einsatz kommen. In Artikel 21 / 4 ist deshalb klar abzugrenzen, ob und inwiefern die Fernmeldediensteanbieter und ISP im Auftrag des zentralen Dienstes bereits entwickelte Spionageprogramme einzusetzen hätten.

Den Einsatz von „Bundes-Trojanern“ lehnen wir klar ab.

Art. 22 Identifizierung von Internet-Benutzern

Fernmeldedianstanbieterinnen und ISP müssen die notwendigen technischen Vorkehrungen treffen, um die Personen identifizieren zu können, die über ihre Vermittlung Zugang zum Internet erhalten.

Angesichts der weiter fortschreitenden technologischen Entwicklung ist hier klar zu definieren und auch abzugrenzen, wie hoch der Aufwand zur Identifizierung sein darf. Bei den als kritisch betrachteten Anwendungsbeispielen wie (drahtlose) Internet-Zugänge in Schulen, Spitälern, Hotels, Restaurants, Internet-Cafés ist ein Vorbehalt anzubringen betreffend der Fähigkeit der Access-Provider, die Identität des Benutzers des Internet-Zugangs in jedem Fall feststellen zu können. Zudem sind die anfallenden Kosten entsprechend der Gebührenverordnung zu entschädigen.

Art. 23 Datenaufbewahrung

Die Kommunikationsdaten (nicht die Inhaltsdaten) über den Fernmeldeverkehr sind von den Fernmeldedianstanbieterinnen und ISP neu während zwölf Monaten aufzubewahren. Die vorsätzliche Verletzung dieser Aufbewahrungspflicht ist neu mit Strafe bedroht.

Wir unterstützen diese Bestimmung, weisen aber auf den zusätzlichen Aufwand hin.

Art. 25 Information über Technologien und Dienste

Fernmeldedianstanbieterinnen und ISP müssen den zentralen Dienst auf dessen Anfrage jederzeit ausführlich über die Art und Merkmale von Technologien und Diensten unterrichten, welche sie der Öffentlichkeit zur Verfügung gestellt haben oder stellen werden.

Hier ist explizit zu ergänzen und festzuhalten, dass der Anbieter bei solchen Auskünften davor bewahrt wird, Geschäfts- und Betriebsgeheimnissen der Fernmeldedianstanbieterinnen und ISP preisgeben zu müssen.

Art. 30 Kosten und Gebühren

Wir sind mit dem Vorschlag, die Kosten einer Überwachung gehen zu Lasten der Personen, welche die Überwachung nach dem Gesetz ausführen, nicht einverstanden.

Die Kosten für die Überwachung müssen wie heute durch die Untersuchungsbehörden im Sinn einer Gebührenordnung abgegolten werden. Art. 30 ist wie folgt umzuformulieren:

¹ Die Kosten der für eine Überwachung notwendigen Einrichtungen und die Kosten der einzelnen Überwachung gehen zu Lasten der die Überwachungen anordnenden Behörde.

² Die anordnende Behörde bezahlt dem Dienst eine Gebühr, welche die Entschädigung zugunsten der die Überwachung durchführenden Anbieterin enthält. Der Bundesrat setzt die Gebühren und Entschädigungen für die Dienstleistungen des Dienstes sowie der verpflichteten Anbieterinnen fest.

Seite 7/7

Art. 34 Rechtsschutz

Wir bitten Sie, den vorgesehenen Gesetzesartikel wie folgt zu formulieren:

¹ Verfügungen des Dienstes unterliegen der Beschwerde nach den allgemeinen Bestimmungen über die Bundesrechtspflege.

² Mit der Beschwerde gegen die Verfügung des Dienstes kann nicht geltend gemacht werden, die Anordnung einer Überwachung sei im konkreten Einzelfall unverhältnismässig oder die anordnende Behörde habe ihr Ermessen unrichtig ausgeübt.

Wir danken Ihnen für die Berücksichtigung unserer Änderungsvorschläge.

Zur Klärung offener und weiterführender Fragen stehen wir jederzeit zu Ihrer Verfügung.

Freundliche Grüsse

Open Systems AG



Martin Bosshardt

Chief Executive Officer



Ogi Stanovcic

Chief Business Officer