

Bundesamt für Justiz
Direktionsbereich Strafrecht
Bundesrain 20
3003 Bern

Bern, 18. August 2010

Stellungnahme zur Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs

Sehr geehrter Herr Rohner

Sehr geehrte Damen und Herren

Für die Möglichkeit, zur Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs Stellung nehmen zu können, danken wir Ihnen bestens.

1. Grundsatz

Das totalrevidierte BÜPF soll die weitreichende Überwachung und die ausgeweitete Speicherung von Daten von unverdächtigen Personen – also nahezu allen Konsumentinnen und Konsumenten – ermöglichen. Zudem soll mit dem Einsatz eines staatlichen «Trojaners» schädliche Software in private Computer eingeschleust werden. Gleichzeitig werden aber die Überwachungsaufgaben nur unklar beschrieben und es bestehen keine Rechtsmittel, sich gegen die Überwachungsanordnungen zur Wehr zu setzen. Weiter wird verlangt, dass diejenigen, welche die Überwachungen im Auftrag des Staates durchführen, die Kosten davon zu tragen haben, und nicht der Staat.

Es wäre zu erwarten gewesen, dass solch weitreichende Änderungen entsprechend begründet werden. Doch dem ist nicht so. Es fehlen in den Vernehmlassungsunterlagen statistisch erhärtete Übersichten, beispielsweise wie viele Anschlüsse wie lange überwacht wurden. Weiter fehlen Informationen, wie effektiv diese Überwachung ist, also ob sie den Strafverfolgungsbehör-

den im Kampf gegen Verbrechen dienen. Schliesslich fehlt eine Übersicht über die Kosten, welche dem Staat anfallen.

Ebenso stossend ist, dass nahezu keinerlei Aussagen über die wirtschaftlichen Folgen des vorliegenden Entwurfs gemacht werden. Dies ist bei derartigen Gesetzesänderungen üblich. Im vorliegenden Fall ist diese Unterlassung besonders gravierend, da zahlreiche Änderungen eindeutige wirtschaftliche Auswirkungen haben, so der Wegfall der Entschädigungspflicht, die Pflicht zum Einschleusen von schädlicher Software in private Computer und die Ausweitung der Überwachungspflicht auf kleine und mittlere Unternehmen und Institutionen wie Hotels, Schulen und Internetcafés.

Die SKS weist die Totalrevision des BÜPF daher zur Überarbeitung zurück. Ein derart unverhältnismässiger Eingriff in die Privatsphäre ist nicht tolerierbar. Eine Neuauflage des totalrevidierten BÜPF soll erstens klar die wirtschaftlichen Folgen darstellen, zweitens mit klaren Auflagen dem Schutz der Privatsphäre unverdächtiger Personen nachkommen und drittens Rechtsmittel vorsehen.

2. Haltung zu den einzelnen Artikeln

Art. 2 Persönlicher Geltungsbereich

Mit dem neuen BÜPF sollen neben den Fernmeldediensteanbieterinnen (FDA) weitere Unternehmen und Personen verpflichtet werden, Überwachungen vorzunehmen. Im Besonderen:

- Hosting-Provider: Webmail-Dienste, Voice-over-Internet-Dienste, Chatrooms, Internetforen und dergleichen
- Betreiber von Internetcafés sowie Hotels, die ihren Gästen, oder Schulen, die ihren Schülerinnen und Schülern Zugang zu einem WLAN gewähren

Damit kommen auf diese Gruppen von Unternehmen und Personen massiv höhere Aufwände zu (siehe auch Art. 22). Dies ist nicht vertretbar. Zudem nimmt damit die Menge der Daten, die zur Identifizierung und zur rückwirkenden Erfassung der Randdaten aufbewahrt werden müssen, enorm zu. Wie im 1. Kapitel erwähnt, ist es unerhört, dass die Auswirkungen auf diese Gruppen nicht einmal dargestellt werden.

Die SKS lehnt daher die Ausweitung der Überwachungspflicht auf diese Gruppen ab.

Art. 15 Allgemeine Aufgaben der Überwachung

Die Formulierung von Buchstabe a ist ungenügend – wie sie es bereits bisher in Art. 13 Abs. 1 lit. a. ist. Denn der Dienst der Überwachung hat keinerlei Kompetenzen, sondern amtiert lediglich als Koordinationsstelle zwischen den Strafverfolgungsbehörden und denjenigen, die die Überwachungsaufgaben durchführen müssen. In Buchstabe a fehlt die Kompetenz des Dienstes zu überprüfen, ob bestimmte Arten von angeordneten Überwachungen vom Gesetz überhaupt vorgesehen sind. In der Praxis leitet er lediglich die Anordnungen weiter. Angesichts der stets steigenden Begehren der Strafverfolgungsbehörden ist dies stossend.

Hinzu kommt, dass den Unternehmen und Personen, welche die Überwachungen durchführen, kein Rechtsmittel in die Hand gegeben wird, um gegen die Entscheide des Dienstes vorzugehen. Denn die Beschwerdeinstanz – das Bundesverwaltungsgericht – kann nur Dinge prüfen, welche die Vorinstanz – der Dienst – geprüft hat. Doch dieser hat ja nichts geprüft, sondern lediglich die Anweisungen übernommen.

Angesichts dessen verlangt die SKS eine klare Prüf- und Kontrollfunktion des Dienstes.

Art. 19

Bereits heute ist die Post verpflichtet, Randdaten aufzubewahren. Eine Unmenge an Daten von Adressen und von Absendern wurde erfasst. Dies ist im Zeitalter, indem die Postkommunikation zulasten der elektronischen Kommunikation stetig abgenommen hat, absurd. Nun soll jedoch die Aufbewahrungsfrist gar von 6 auf 12 Monate verdoppelt werden. Die SKS lehnt dies ab, da die gesammelten Daten für die Strafverfolgung kaum praktischen Nutzen haben.

Art. 21 Pflichten bei der Durchführung von Überwachungen

Zwar werden mit Art. 21 erstmalig die Pflichten der Überwachung zusammengefasst, also es wird teilweise geregelt, welche Überwachungsaufgaben wahrzunehmen sind. Doch sind diese Pflichten einerseits weiterhin zu ungenau geregelt, andererseits gehen sie zu weit. Neben Abs. 4 (siehe nächster Abschnitt) betrifft Letzteres insbesondere die beliebige Pflicht zur Aussonderung von bestimmten Daten aus dem zu liefernden Datenstrom (Abs. 3). Dies ist technisch nicht möglich.

Es ist daher zwingend, die Pflichten zu limitieren. Dies ist nicht nur im Interesse derjenigen, die Überwachungen durchführen, sondern klar im Interesse der Konsumentinnen und Konsumenten.

ten. Wenn die Pflichten klar definiert sind, können nicht willkürlich Arten der Überwachung angeordnet werden, da das Gesetz dann endlich einen konkreten Rahmen vorschreibt.

Ursprünglich wurde in den kantonalen Strafprozessordnungen die Telefonüberwachung festgeschrieben. Damals war klar, was Telefonüberwachung ist und was die Pflichten der PTT waren. Heute aber, mit dem technischen Fortschritt, werden zahlreiche Überwachungen verlangt, welche keine klaren gesetzlichen Grundlagen haben. Angesichts der Nutzung von Mobiltelefonen und Internet geht es häufig um Ortungsfunktionen und Rasterfahndungen. Bei letzteren wird überwacht, wer in einem bestimmten Aufenthaltsgebiet welche Verbindungen getätigt hatte. Gerade dies ist bedenklich, da es nicht mehr darum geht, eine verdächtige Person zu überwachen, sondern generell Daten zu sammeln. Dies ist nicht im Sinn der Strafprozessordnung.

Die SKS verlangt daher die Festschreibung von klaren Pflichten in Art. 21, die zudem technisch machbar sind und sich auf die Überwachung Verdächtiger zu konzentrieren haben.

Art. 21 Abs. 4 und StPO Art. 270^{bis}

Was sich hinter unscheinbaren Begriffen wie «Onlinedurchsuchung» oder «Einschleusung von Informatikprogrammen» verbirgt, ist nichts anderes als das Einbauen von Schaden anrichtender Software in die Computer von Privatpersonen, ohne dass deren Inhaber davon Kenntnis haben. Diese Massnahme soll mit der Änderung der Strafprozessordnung in Art. 270^{bis} eingeführt werden.

Eingeschleust werden sollen Trojaner, Spyware und dergleichen, also Software, vor der ansonsten gewarnt wird und vor denen Antivirus- und Antispyprogramme schützen. Mit dem neuen Artikel sollen also die Überwachungsbehörden das Recht haben, solche schädlichen Programme einzuschleusen bzw. die FDA zu verpflichten, diese Programme einzuschleusen.

Damit verbunden ist ein massiver und einmaliger Eingriff in die Privatsphäre der Konsumentinnen und Konsumenten. Denn sie nutzen den mit dem Internet verbundenen PC für alle möglichen Zwecke, z.B. zur Kommunikation, zur Speicherung privater Kommunikation wie Bewerbungsschreiben oder privater Fotos etc. Die gewonnenen Informationen sind daher äusserst persönlich.

Weiter könnte es möglich sein, dass der staatliche Trojaner beispielsweise alle Passwort-Eingaben nachverfolgen oder auch das Mikrofon eines Laptops unbemerkt anschalten und dadurch alles mithören kann.

Zudem ist zu befürchten, dass diese Methode des Eindringens in private Computer eine Sicherheitslücke schafft, die irgendwann auch von Verbrechern genutzt werden kann. So ist möglich,

dass die Quellsoftware des staatlichen Trojaners im Netz auftaucht und von Verbrechern missbraucht wird.

Weiter ist zu erwarten, dass diejenigen, welche mit derlei Massnahmen überwacht werden sollen, ausweichen. Sie könnten Vorsichtsmassnahmen treffen oder andere Kommunikationskanäle als ihren eigenen Computer nutzen. Damit trifft die Überwachungsmassnahme genau die ahnungslosen und unverdächtigen Konsumentinnen und Konsumenten.

Schliesslich ist eine derartige Verpflichtung von Unternehmen, Polizeiaktionen durchzuführen, im schweizerischen Recht einmalig.

Aus all diesen Gründen lehnt die SKS Art. 270^{bis} StPO und Art. 21 Abs. 4 BÜPF entschieden ab.

Art. 22 Identifizierung von Internet-Benutzern

In Kombination mit Art. 2 müssen gemäss Art. 22 Internetcafés, Schulen, Hotels und andere, die zum Beispiel über ein WLAN Zugang zum Internet ermöglichen, gemeinsam mit den Providern alle Personen identifizieren, die an ihren Stationen ins Internet gehen. Als mögliche Massnahme schlägt das BJ vor, den Internetzugang erst nach Angabe einer Handynummer zu gewähren.

Im Bericht geht das BJ nicht darauf ein, was die Konsequenzen für die genannten Gruppen sind. Wie im 1. Kapitel erwähnt, ist dies schlicht rücksichtslos. Die genannte Massnahme führt zu bedeutenden Mehrkosten. Aufgrund dieser Kosten werden sich die genannten Gruppen zwei Mal überlegen, ob sie einen solchen Internetzugang anbieten wollen. Im Endeffekt bedeutet dies, dass Schulen, Internetcafés, Hotels und dergleichen weniger die Möglichkeit anbieten, ins Internet gehen zu können. Damit drohen die Art. 2 und 22, den öffentlichen Zugang zum Internet zu reduzieren! Diese Massnahme ist im heutigen Zeitalter schlicht technologie- und fortschrittsfeindlich.

Angesichts dessen lehnt die SKS den Art. 22 ab.

Art. 23 Datenaufbewahrung

Mit Art. 23 werden Daten unverdächtiger Personen auf Vorrat gespeichert. Die skandalöse Regelung des Festhaltens der Kommunikation aller Privater wird damit im neuen BÜPF weitergeführt. Dies ist umso unverständlicher, als die Geschäftsprüfungsdelegation Ende Juni Zweifel an der Richtigkeit und Relevanz der Daten der ISIS-Datenbank äusserste. Denn es seien mehr als 200'000 Daten gesammelt. So werden in der überwiegenden Mehrheit unverdächtige Personen registriert ohne Nutzen für die Strafverfolgung.

Die vorgeschlagene Verlängerung der Aufbewahrung von 6 auf 12 Monate verschärft die Problematik. Die SKS lehnt die Verlängerung daher ab.

Art. 30

Neu sollen die Kosten der Überwachung nicht mehr vom Bund getragen werden, sondern von jenen, welche die Überwachung durchführen. Die SKS lehnt dieses Ansinnen entschieden ab.

Erstens ist nicht einzusehen, warum der Staat seine Aufgaben im Sinn der Strafverfolgung nicht selbst finanziert, wie dies üblich ist. Da die Überwachenden die Rolle von Hilfspolizisten übernehmen, sticht die Begründung, es bestehe wie bei den Banken eine Editionsspflicht, nicht. Auch Hilfspolizisten sind vom Staat zu entschädigen.

Zweitens würde mit der Überwälzung der Kosten eine massive Belastung der Überwachenden entstehen. Gemäss Angaben der Internetprovider belaufen sich die jährlichen Kosten der Überwachung auf durchschnittlich 9 Millionen Franken. Gerade für kleinere Unternehmen als auch für die im vorgängigen Abschnitt benannten Gruppen sind diese Kosten nicht tragbar und bedeuten eine Gefährdung ihrer wirtschaftlichen Existenz.

Drittens werden diese Kosten noch in besonderem Masse ansteigen. Erstens weil mehr Überwachungen stattfinden. Zweitens weil neu die Überwachenden eine Schadsoftware in die Datenverarbeitung ihrer Kundinnen und Kunden einschleusen müssen. Diese Kosten werden immens sein, wie die Branche befürchtet.

Viertens ist zu erwarten, dass diese Kosten schliesslich auf die Konsumentinnen und Konsumenten überwälzt werden.

Fünftens – und diesem Aspekt muss besondere Bedeutung zugemessen werden – verändert sich damit die Anreizstruktur, Überwachungen anzuordnen. Wenn der Staat die Kosten nicht tragen muss, können ohne Berücksichtigung der wirtschaftlichen Folgen Überwachungen angeordnet werden. Somit wird tendenziell zu viel überwacht. Wenn hingegen der Staat die Kosten selber tragen muss, besteht der Anreiz, haushälterisch mit Überwachungsanordnungen umzugehen. In einer separaten Rechnung wird dann klar, wie viel die Überwachungskosten betragen und ob dieser Aufwand tatsächlich vertretbar ist.

Art. 31 Übertretungen

Die Strafbestimmung ist eindeutig zu strikt. Dies insbesondere deshalb, weil diejenigen, welche Überwachungen durchführen, kaum Mittel haben, dem Einhalt zu gebieten (siehe Art. 15). Aufgrund dessen und der Tendenz, immer mehr Überwachungen durchzuführen, führt die Strafbestimmung dazu, dass die FDA willkürlich den Anordnungen unterworfen sind.

Zudem wird die Strafhöhe gerade kleinere Provider existenziell bedrohen.

Die SKS verlangt daher eine deutlich abgeschwächte Formulierung.

Art. 270^{ter} StPO Einsatz von Ortungsgeräten

Der neue Art. 270^{ter} der Strafprozessordnung erlaubt den Einsatz von so genannten IMSI-Catchern. Diese Geräte suggerieren den im Umfeld befindlichen Mobiltelefonen, es sei eine Mobilfunkantenne, womit sie den Mobilfunkverkehr der entsprechenden Mobiltelefone auf sich ziehen. So können die Mobiltelefone anhand der IMEI- und SIM-Kartenummer identifiziert werden. Damit wird bei allen Personen im Umkreis – verdächtige und unverdächtige – der Mobilfunkverkehr gestört. Dies ist nicht zu verantworten.

Ausserdem ist zu befürchten, dass die IMSI-Catcher schliesslich hierfür eingesetzt werden, um zu eruieren, wer sich an einem bestimmten Ort aufhält oder um gezielt den Telefonverkehr zu stören. Erfahrungen im Ausland bestätigen diese Befürchtung.

Die SKS lehnt daher Art. 270^{ter} ab.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Mit freundlichen Grüssen
STIFTUNG FÜR KONSUMENTENSCHUTZ

sig.

Sara Stalder
Geschäftsleiterin

sig.

Andreas Tschöpe
Leiter Politik und Wirtschaft