



Bundesamt für Justiz
Direktionsbereich Strafrecht
Bundesrain 20
3003 Bern

18. August 2010

Vernehmlassung zur Änderung des BÜPF Stellungnahme der Piratenpartei Schweiz

Sehr geehrte Damen und Herren

Die Piratenpartei Schweiz (PPS), im Juli 2009 gegründet, zählt 900 Mitglieder. Sie setzt sich für die «digitale Generation» ein und nimmt gerne die Gelegenheit wahr, zur Revision des Bundesgesetzes betreffend der Überwachung des Post- und Fernmeldeverkehrs (BÜPF) Stellung zu nehmen. Gerade Regelungen im Post- und Fernmeldeverkehr, insbesondere aber im Internet, zählt zu den Kernkompetenzen (der Partei, für die Freiheit eines der wichtigsten Güter darstellt).

Allgemeine Bemerkungen

Das Internet ist nicht als Ausnahmebereich zu sehen, sondern als integraler Bestandteil unserer Gesellschaft. Selbstverständlich müssen in allen Lebensbereichen Regeln gelten, die durch Gesetze festzuhalten sind. Es gilt aber im Gegenzug, unsere Grundrechte wie die Privatsphäre und die Meinungs- und Informationsfreiheit entschieden zu bewahren. Dazu gehört im erweiterten Sinn der freie Zugang zu Wissen und Kultur, ein transparenter Staat und der absolute Verzicht auf Zensur. Auf dieser Grundlage basiert die nachfolgende Stellungnahme und konkrete Kritik zur BÜPF-Revision.

Art. 1 Sachlicher Geltungsbereich

Beim Geltungsbereich wird davon gesprochen, dass das neue BÜPF für den Post- und Fernmeldeverkehr, "einschliesslich des Internetverkehrs", gilt. Dabei wird suggeriert, dass das Internet ein Teil des Post- und Fernmeldeverkehrs ist, weil es ja explizit eingeschlossen und nicht gleichrangig erwähnt wird. Dass dies Kontrovers ist, kann nicht bestritten werden, denn sonst wäre die explizite Erwähnung ja sinnlos. Den umfassenden Begriff "Internet" als Teil des Post- und Fernmeldeverkehrs ins BÜPF einzuführen, zeugt vom Unverständnis für dieses



Medium sui generis. Das Internet ist eben kein erweitertes Telefon und auch kein erweitertes Fax. Es ist ein neues Medium, das die Funktion und Nutzung in allen angrenzenden Bereichen paradigmatisch verändert. Deshalb herrscht ja ein Anpassungsdruck auf das BÜPF. Es ist zu vermuten, dass Art. 1 implizit nur gewisse Aspekte des Internets als sachlichen Geltungsbereich ansieht, wie die Internettelefonie oder den E-Mail-Verkehr, jedoch nicht hoch sensible Systeme wie die Interbankenkommunikation, Luftraumüberwachung, Energieversorgungssicherung, die technisch gesehen Internetverkehr darstellen. Die Spezifikation "Internetverkehr" ist unzureichend.

Art. 2 *Persönlicher Geltungsbereich*

Erklärtes Ziel des neuen BÜPF ist es, den persönlichen Geltungsbereich genauer zu formulieren und zu ergänzen. Nun scheint zweiteres im Vordergrund zu stehen, denn von einer genaueren Formulierung kann nicht die Rede sein. Art. 2 Abs. 1 hat zur Folge, dass alle Personen, deren berufsmässige Tätigkeit mit dem Internet zu tun hat, Überwachung im Sinne des BÜPF durchführen müssen. Also nicht nur Internet-Anbieterinnen, sondern auch Webhoster und Service-Provider. Überwachung dulden müssen faktisch alle, die Internetzugang haben, weil das Internet gerade daraus besteht, Kommunikationsdaten zu verwalten und an dritte Weiterzuleiten. Es gibt keinen Nutzer und keine Nutzerin des Internets, die die Bedingungen in Art. 2 Abs. 2 BÜPF (Duldung der Überwachung) nicht erfüllen. Jeder Betreiber eines LANs (inklusive Privatpersonen) muss eine Überwachung seitens des ISPs dulden. Ob darunter eine Überwachung des Datenverkehrs nach aussen oder LAN-intern gemeint ist, bleibt offen. Der Gesetzestext ist darin ungenau formuliert.

Art. 6 *Grundsatz*

Das Informatiksystem des Dienstes wird als Werkzeug zur Verarbeitung der durch die Überwachung gewonnenen Daten definiert. Jedoch hat der Dienst auch die Aufgabe der Infiltrierung von Datensystemen gemäss Art. 270bis (neu) StPO. Sofern die Einschleusung von Informatikprogrammen Teil des Informatiksystems ist, so bedarf Art. 6 als Grundsatz eine Erweiterung um die Bearbeitung von überwachten Datensystemen. Es werden ja nicht nur Daten verarbeitet, die aus der Überwachung des Fernmeldesystems gewonnen wurden, sondern auch deren Quelle.

Falls das Infiltrationssystem ein eigenes System unabhängig des Verarbeitungssystems darstellt, so braucht es eine eigene Definition und gesetzliche Grundlage.



Art. 10 *Akteneinsichtsrecht und Auskunftsrecht über die Daten*

Abs. 4 gewährt der von Überwachung betroffenen Person ein Auskunftsrecht über die gewonnenen Daten. Dieses Recht muss jedoch bei der mit dem entsprechenden Fall befassten Behörde eingefordert werden. Es kann nicht direkt beim Dienst geltend gemacht werden. Dies ist insbesondere problematisch, wenn die Überwachung verdeckt durchgeführt wird und eine Mitteilung entsprechend Art. 279 Abs. 2 StPO unterlassen wird. Es wird zu einem Recht ohne Adressaten.

Art. 11 *Aufbewahrungsfrist von Daten*

Abs. 1 setzt die Aufbewahrungsfrist bis zur Strafverfolgungsverjährung fest. Dass mit dem Auslaufen dieser Frist die Daten gelöscht werden müssen, sollte erwähnt sein.

Abs. 2 regelt die Aufbewahrungsfrist bei Rechtshilfeersuchen. Für die Fristen sollten nicht die Erforderlichkeiten der verfolgten Ziele entscheidend sein, sondern die Verjährung.

Art. 12 *Sicherheit*

Nicht nur der Dienst und die Überwachung durchführenden Personen müssen der Vorschriften über technische und organisatorische Schutzmassnahmen unterstellt werden, sondern auch die das Verarbeitungssystem nutzenden Behörden und die von ihnen bestimmten Dienststellen.

Art. 15 *Allgemeine Aufgaben der Überwachung*

Als allgemeine Aufgabe des Dienstes fehlt die Erstellung und Wartung eines Infiltrationssystems. Gemäss Art. 270bis StPO ist die Staatsanwaltschaft befugt, eine Überwachung mittels eines Informatikprogramms anzuordnen, welches ohne Wissen der betroffenen Person in ihr Dateisystem eingeführt wird. Diese geheime Überwachungsmassnahme kann nur in Zusammenarbeit mit den entsprechend diesem Gesetz Überwachung durchführenden Personen geleistet werden. Folglich ist der Dienst verantwortlich und nur er kann die entsprechende Infiltrationssoftware zur Verfügung stellen. Denn gemäss Art. 21 Abs. 4 dieses Gesetzes leisten die Überwachung durchführenden Personen nur die nötige Unterstützung, um Informatikprogramme in das Datensystem einzuschleusen. Die Herstellung und Wartung von Infiltrationsprogrammen ist aber keine blosser Unterstützung. Der Dienst muss zwingend für die Herstellung und Wartung des Infiltrationssystems zuständig sein.

Art. 18 *Zertifizierung*



Der Staat ordnet eine Zertifizierungspflicht an, gleichzeitig sollen die Internetdienstleister aber dafür bezahlen, dass er überprüft, ob sie sich an ein Gesetz halten. Wir erachten dies als unverhältnismässige Belastung der Internetdienstleister. Siehe auch den Kommentar zu Artikel 30.

Artikel 19 Abs. 2 und Art. 23 Datenaufbewahrung

Es ist uns trotz Erläuterungen im Bericht unverständlich, warum Randdaten in Zukunft doppelt so lange gespeichert sein sollen. Es muss nicht von mehreren Monaten für die Eröffnung eines Verfahrens ausgegangen werden, wengleich dem die Motion 06.3170 von Rolf Schweizer entgegen hält. Eine Verdoppelung der Aufbewahrungsdauer bedeutet ausserdem auch eine Verdoppelung der anfallenden Daten. Das bedeutet auch, dass doppelt so viele Speichermedien konstant für deren Speicherung reserviert sein müssen. Die resultierenden Kosten dürfen nicht unterschätzt werden.

Art. 21 Pflichten bei der Durchführung von Überwachungen

Abs. 2 legt fest, dass Verbindungs-, Verkehrs- und Rechnungsdaten "so rasch als möglich" und der Fernmeldeverkehr der überwachten Person "soweit möglich in Echtzeit" geliefert werden sollen. Diese Unverzüglichkeit bzw. Echtzeit sind für die Überwachung durchführenden Personen ein grosser Kostenfaktor, der mit dem Nutzen für die Strafverfolgung in keinem Verhältnis steht. Die Übermittlung von Aufzeichnungen ist für die Verwertung als strafrechtlich relevantes Material vollauf genügend. Bei Gefahr in Verzug ist keine Überwachung anzusetzen, sondern der sofortige Zugriff durchzuführen. Der ermittlungstaktische Vorteil einer Echtzeitüberwachung ist nicht einzusehen, wenn diese Überwachung verdeckt durchgeführt wird.

Art. 22 Identifizierung von Internet-Benutzern

Durch diesen Artikel kann von einem Zugangsanbieter verlangt werden, dass nicht nur der Anschlussinhaber, sondern auch Freunde und Bekannte identifiziert werden müssen. Das bedeutet, dass eine individuelle Zugangsidentifikation durch den Internetanbieter vorgeschrieben wird. Konsequenter Weise muss sich dann jeder Internetnutzer mit einem persönlichen Passwort einloggen und die kollektive Nutzung eines Internetzugangs wäre eine Verletzung der zukünftigen Nutzungsbestimmungen der Internetanbieter. Dieser Artikel hat damit gravierende Auswirkungen auf den täglichen Umgang aller Internetnutzer.



Art. 30

Gemäss Abs. 1 sollen die Internetanbieter die obligatorischen Überwachungsmassnahmen selber finanzieren. Gleichzeitig erhält die anordnende Behörde nach Absatz 2 weiterhin die bisherige Gebühr ausgezahlt. Das Argument, dass Internetanbieter Überwachungsmassnahmen gemäss diesem Gesetz durchführen, ohne finanziell dafür entschädigt zu werden, weil sie damit vom Kampf gegen den Missbrauch ihres Dienstes profitieren, ist nicht stichhaltig. Die Kosten durch geleistete Überwachung sind für die Anbieter reell sehr hoch, während der Nutzen fiktiv ist. In Wirklichkeit ist dies eine Überwälzung der Strafverfolgungskosten auf die Privatwirtschaft. Besonders kleine und mittlere Unternehmen geraten deswegen in Existenzschwierigkeiten.

StPo Art. 270bis Der Bundestrojaner

Die Bezeichnung "Abfangen und Entschlüsselung von Daten" ist irreführend, da es faktisch um das Einschleusen eines Trojaners in das zu überwachende System geht. Methoden der Geheimdienste halten damit Einzug in die Strafverfolgung. Drei Punkte sind dabei besonders zu Bemängeln:

1. Das Einschleusen eines Informatikprogrammes in das Datensystem ohne Wissen der überwachten Person kommt einer geheimen Hausdurchsuchung gleich. Es ist eine aktive Massnahme, im Gegensatz zu einer passiven Telefon- oder Postüberwachung, denn das Einschleusen des Informatikprogramms ist eine Manipulation des Datensystems. Das Informatikprogramm, genauer der Trojaner, soll das Datensystem dermassen verändern, dass Daten an den überwachenden Dienst weitergeleitet werden. Aktive Massnahmen müssen der betroffenen Person stets Rechtmittel zugestehen.
2. Das Einschleusen eines Informatikprogrammes soll erst angewendet werden, wenn bisherige Massnahmen erfolglos blieben, andere Massnahmen aussichtslos oder die Überwachung unverhältnismässig erschweren würden. Damit wird suggeriert, dass das Einschleusen eines Trojaners erst das letzte Mittel ist, wenn alle anderen versagt haben oder untauglich sind. Wenn bisherige Ermittlungsmethoden versagt haben, liegt es natürlich nahe, weitergehende Mittel einzusetzen. Doch geht die Überlegung, dass der Verdächtige vielleicht unschuldig ist, dabei unter. Diesem Umstand soll die Notwendigkeit einer Genehmigung durch das Zwangsmassnahmengericht entgegenwirken. Jedoch ist fraglich, ob das Zwangsmassnahmengericht die technische Kompetenz hat, das Ausmass des Eingriffs in die Privatsphäre durch das Informatikprogramm einzuschätzen. Die Überwachungstrojaner müssen spezifisch für das zu infiltrierende Datensystem hergestellt oder angepasst werden. Das Zwangsmassnahmengericht benötigt die technische Kompetenz um die Risiken für das Datensystem einschätzen zu können. Ansonsten muss es sich auf die Fachkompetenz



des Überwachungsdienstes verlassen, was die Idee der institutionellen Kontrolle ab absurdum führt.

3. Das Einschleusen eines Informatikprogrammes in ein fremdes Datensystem nimmt die Beschädigung dieses Systems in Kauf. Der genaue Zustand des zu infiltrierenden Datensystems ist nicht bekannt, sonst wäre die Überwachung ja sinnlos. Die Interaktion des Überwachungstrojaners mit anderen Elementen des Datensystems kann vorgängig nicht exakt bestimmt werden. Daraus ergeben sich Risiken für das betroffene Datensystem, wie auch für dritte. Die Frage nach der Haftung für beschädigte oder kompromitierte Datensysteme bleibt offen.

Der Trojaner selber stellt auch eine potenzielle Sicherheitslücke dar, die irgendwann von "Bösen" missbraucht wird. Denn eins ist sicher: Der "Standardbündestrojaner" wird rasch im Netz verbreitet sein und somit jedem für Überwachungen zur Verfügung stehen.

Schlussbemerkungen

Gestützt auf diese Betrachtungen lehnt die Piratenpartei die Änderungen des BÜPF grundlegend ab und spricht sich für die Überarbeitung im Sinne der obigen Stellungnahme aus. Sie warnt vor einer überhasteten Einschränkung der Grundrechte ohne grundsätzliche Nachforschungen. Ferner betrachtet sie die Vorratsdatenspeicherung als eine inakzeptable und anlasslose Erfassung von zum Teil höchst sensiblen Daten. Anrufe zu Ärzten, Anwälten, Journalisten, der dargebotenen Hand und anderen intimen Gesprächspartnern gehen im Sinne der Bundesverfassung (Art. 13 Abs. 1) den Staat nichts an. Schliesslich sind automatisch analysierte Verbindungsdaten aussagekräftiger als Sammlungen von Inhaltsdaten.

Grundsätzlich ist die Verhältnismässigkeit der Überwachung aller Personen gegenüber dem resultierenden Sicherheitsgewinn nicht gegeben. Die Freiheiten und Rechte der Menschen sind stets höher zu werten. Mit der Vorratsdatenspeicherung wird aber faktisch jeder und jede verdachtsunabhängig überwacht. Diese Speicherung hebt die Unschuldsvermutung aus – jede Person wird als potentieller Terrorist gebrandmarkt.

Wir bedanken uns für die Berücksichtigung unserer Anmerkungen.

Mit freundlichen Grüssen

Denis Simonet
Präsident

Pascal Gloor
Vizepräsident

