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, Anschaffung 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 Einwählda ten 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 Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) der Swiss Privacy Foundation vom 16. August 2010 (Kapitel 8, https://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 e zienten 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) Identifizierung 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.