Stellungnahme der Digitalen Gesellschaft zum Entwurf des Bundesrats für ein totalrevidiertes Bundesgesetz betreffend die Überwachung des Post und Fernmeldeverkehrs (BÜPF) (Botschaft vom 27. Februar 2013)

Digitale Gesellschaft
www.digitale-gesellschaft.ch

unterzeichnet von den Organisationen

Big Brother Awards Schweiz
CCC Schweiz
Digitale Allmend
grundrechte.ch
immerda.ch
Piratenpartei Schweiz
SIUG (Swiss Internet User Group)
Swiss Privacy Foundation
xiala.net

10. März 2013

Trotz breiter Kritik in der Vernehmlassung will der Bund nun in der geplanten Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) den Einsatz von Bundestrojanern rechtlich verankern und die verfassungsrechtlich problematische Vorratsdatenspeicherung massiv ausdehnen.

Eine Studie des Max-Planck-Instituts widerlegt die Behauptung, dass die Vorratsdatenspeicherung zu höheren Verbrechens-Aufklärungsquoten führt. Die Aufklärungsraten in der Schweiz sind deutlich niedriger als jene in Deutschland, wo schon heute deutlich viel weniger Überwachung zulässig ist als hierzulande. Dennoch hält der Bundesrat an einer weiteren Ausdehnung der Überwachung fest.

Die Ausweitung des Geltungsbereichs des Überwachungsgesetzes von 50 Access Provider auf sämtliche private und geschäftliche Anbieterinnen von Online-Diensten stellt eine gravierende Erweiterung der Überwachung dar. Gleichwohl kann das Gesetz nicht auf ausländische Anbieterinnen angewendet werden, womit die Nützlichkeit nicht gegeben ist.

Im Gegensatz zur Schweiz werden in Deutschland Bundestrojaner und Vorratsdatenspeicherung immerhin vom Bundesverfassungsgericht klar kritisiert:

Bereits 2008 hat dieses höchste deutsche Gericht der Online-Überwachung nicht nur enge Schranken auferlegt (die ausschliessliche Überwachung auf Telekommunikationsdaten „muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein“) sondern auch gleich ein neues „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ geschaffen.

Ebenfalls hat das deutsche Bundesverfassungsgericht eine Regelung, die in etwa der heutigen Gesetzeslage zur Vorratsdatenspeicherung in der Schweiz entspricht, mit Urteil vom März 2010 für verfassungswidrig und nichtig erklärt - und die sofortige Löschung der bis an hin gesammelten Daten angeordnet.

1 Vorratsdatenspeicherung

In der Schweiz hingegen wird die Vorratsdatenspeicherung weiter ausgebaut. Mit der Überarbeitung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) Ende 2011 wurde bereits ohne genügende gesetzliche Grundlage und damit unter Umgehung der demokratischen Grundsätze unserer Verfassung die Rasterfahndung per „Antennensuchlauf“ erlaubt. Mit der neuen Botschaft zum Bundesgesetz (BÜPF) soll nun die Vorhaltedauer der Daten von 6 auf 12 Monate ausgedehnt werden.

Betroffen von dieser Massnahme sind ausnahmslos alle EinwohnerInnen der Schweiz, wobei bezogen auf den Grossteil der Bevölkerung nur ein hypotheti-

sches Interesse an den Daten (zur Verfolgung von 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, vorausgehende und rein präventive 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.

Die verdachtsunabhängige Speicherung von Verbindungs-, Verkehrs- und Rechnungsdaten stellt einen schweren Eingriff in die persönliche Freiheit dar. Das verfassungsmässige Fernmeldegeheimnis muss korrekterweise nicht nur garantieren, dass wir alle kommunizieren können, ohne abgehört zu werden, sondern auch, ohne beobachtet zu werden.

Ein Grundrechtseingriff muss immer verhältnismässig (also für die Verfolgung eines öffentlichen Interesses notwendig und dafür geeignet) sein. Eine Studie des renommierten Max-Planck-Institut im Auftrag des deutschen Bundesamtes für Justiz kommt hingegen zum Schluss, dass die Vorratsdatenspeicherung für die effektive Strafverfolgung unnötig ist. Und nicht nur dies: Eine direkte Gegenüberstellung der Aufklärungsquoten in der Schweiz (mit Vorratsdatenspeicherung) und in Deutschland (ohne) aus dem Jahr 2009 zeigt eine ähnliche, in einigen Deliktsbereichen jedoch eine massiv höhere Aufklärungsquote - für Deutschland.

In der Botschaft zum BÜPF werden keine genaueren Angaben dazu gemacht, wieso die Vorratsdaten „zur Bekämpfung der Kriminalität unerlässlich“ sein sollen. Zahlenmaterial fehlt. Fehlt aber der Nachweis der Verhältnismässigkeit, muss die Vorratsdatenspeicherung als eine unrechtmässige Einschränkung der Grundrechte gelten - die nicht angewendet werden darf.

Die Ausdehnung der Speicherpflicht wird damit begründet, dass „diese Frist bereits vollständig oder grösstenteils abgelaufen [ist], wenn die Behörde in der Lage ist, eine Überwachung anzuordnen“. Die Ausdehnung eines bereits unrechtmässigen Grundrechtseingriff wird also damit legitimiert, dass die Strafverfolgungsbehörden zu wenig schnell arbeiten (resp. unter-dotiert sind)! Zahlen dazu gibt es einmal mehr keine.

2 Trojaner Federal (auch Bundestrojaner, Staatstrojaner oder im Behördensprech GovWare genannt)

Der Bundesrat gibt in der Botschaft zu, dass per „GovWare [...] technisch auf sämtliche Daten, beispielsweise auch auf alle privaten Informationen zugegriffen werden (z.B. Dokumente, Fotos) [kann], die in einem Computer gespeichert

sind“. Er will die Verwendung dieser Daten vor Gericht verbieten. Bloss: Die Überwachung beginnt bereits beim Sammeln der Daten - und nicht erst bei der Weiterverwendung. Die Ausführung der Zwangsmassnahme (Einschleusen, die Durchführung der Überwachung und deren Beendigung) ist den Polizeien überlassen, die selber in einem offensichtlichen Interessenkonflikt stehen, weil sie sich die Arbeit gerade auch mit einer über die gesetzlichen Grenzen hinaus gehenden Datenbeschaffung vereinfachen können. Es findet keine unabhängige Kontrolle der Software, des Vorganges oder der gesammelten/ verwerteten Daten statt. Missbrauch werden Tür und Tor geöffnet.

Das deutsche Bundesverfassungsgericht hat sich in seinem Urteil zur Online-Durchsuchung daher klar dahingehend geäussert, dass sich die Überwachung ausschliesslich auf Daten aus einem laufenden Telekommunikationsvorgang beschränken - und dies „durch technische und rechtliche Vorgaben sichergestellt sein“ muss. Der Bundesrat hält solche Vorgaben zum Schutz der BürgerInnen nicht für nötig.

Auch beim Bundestrojaner stellt sich also vorab die Frage der Verhältnismässigkeit. Nicht erst der konkrete Einsatz einer Funktion beschneidet Grundrechte, sondern bereits dessen Möglichkeit. „Es geht nicht um konkret ausgeübte Kontrolle, sondern andersherum um den Kontrollverlust des/r Betroffenen. So müssen sich die technischen Vorgaben im Nichtvorhandensein unzulässiger Funktionalität äussern, nicht im Nichteinsatz unzulässiger, aber vorhandener Funktionalität.“ (Angezapft, Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, Rainer Rehak, 2012)

Das Einbringen des Bundestrojaners in die zu überwachenden Computersysteme soll entweder durch Eindringen in die Räumlichkeiten, in denen sich das System befindet, geschehen, oder dann durch Zusenden eines mit dem Trojaner verseuchten E-Mails. Damit sich die zugesandte Malware in das System einnisten kann, muss es möglicherweise eine AntiViren-Software umgehen und über weit gehende Rechte verfügen, was meist nur durch Ausnutzung einer Sicherheitslücke möglich ist. Dabei stellen sich einige Fragen:

- Darf eine vorhandene AntiViren-Software deaktiviert werden, mit dem Risiko, dass die NutzerInnen nachher auch durch Dritte, kriminelle Elemente, geschädigt werden?
- Woher nimmt sich die zuständige Polizeibehörde die Information über die für das Eindringen in Computersysteme nötige Sicherheitslücke? Darf sie sich einen solchen „Exploit“ auf dem Schwarzmarkt beschaffen? Wäre die Polizei nicht vielmehr zuständig, auf Sicherheitslücken aufmerksam zu machen, anstatt diese selber zu nutzen und der Kriminalität noch Vorschub zu leisten?
- Wie wird sichergestellt, dass nur die Kommunikation von der tatsächlich zu überwachenden Person aufgezeichnet wird, insbesondere wenn sich

mehrere Personen einen Computer teilen?

- Was bedeutet die Überwachung des „Inhalts der Kommunikation“? Betrifft dies eine E-Mail, die heute geschrieben, gespeichert und morgen anstatt zu versenden gelöscht wird? Und wenn sie schon heute verschlüsselt wird? Wann also beginnt die „Kommunikation“?
- Die Aufzeichnung eines Video-Chats ist immer auch eine Wohnraumüberwachung (dessen, was im Hintergrund geschieht).
- Wie wird die nötige Beweissicherheit für die Verwendung vor Gericht auf einem fremden und entfernten System gewährleistet?
- Wie wird die (rückstandsfreie) Entfernung der Software gewährleistet?

Leider blendet die Botschaft all diese Punkte schlicht aus. Der Bundesrat hält einzig fest: „Das vorrangige Ziel der Revision des BÜPF besteht nicht darin, vermehrt zu überwachen, sondern die Überwachungsmethoden an die technische Entwicklung im Fernmeldebereich anzupassen. Dieses Ziel lässt sich nach Ansicht des Bundesrates nur erreichen, wenn den Strafverfolgungsbehörden gestattet wird, GovWare einzusetzen. Andernfalls würde die Wirksamkeit der Kriminalitätsbekämpfung sehr stark beeinträchtigt.“

Wie schon oben bemängelt, bleibt er auch hier den Nachweis der Wirksamkeit der geplanten Massnahmen schuldig.

3 Erweiterter Geltungsbereich des Gesetzes

Stehen nach dem bisherigen Gesetz klar und ausdrücklich nur die Access Provider in der Pflicht, die Überwachungsmassnahmen vorzunehmen, sollen neu auch reine E-Mail-Anbieterinnen, Hostingprovider, Hotels, Spitäler, Schulen, Chatanbieterinnen und Private, die ihr WLAN auch den Nachbarn zur Verfügung stellen, etc. unter das BÜPF fallen. Sie müssen „eine Überwachung [...] durch den Dienst oder durch die von diesem beauftragten Personen dulden“. Und dazu „unverzüglich Zugang zu ihren Anlagen gewähren“ und „die für die Überwachung notwendigen Auskünfte erteilen“. Was mit „Anlagen“ gemeint ist, bleibt höchst unklar. Wie wird gewährleistet, dass auch tatsächlich nur die von der Überwachungsmassnahme betroffene Person überwacht wird?

Mit dieser Ausweitung des Geltungsbereichs auf sogenannte „Anbieterinnen abgeleiteter Kommunikationsdienste“ sollen sich Tausende kleine Anbieterinnen von Internetdiensten, die einen Mailserver für ein paar Freunde oder ein Forum für den lokalen Tischtennisverein betreiben zu Gehilfen des Überwachungsstaats machen.

Der Bundesrat behält sich zudem vor, „alle oder einen Teil der Anbieterinnen [...], die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder

für eine grosse Benutzerschaft anbieten, allen oder einem Teil der“ generellen Überwachungspflichten zu unterstellen. Er gibt sich damit auch das Recht, darüber zu bestimmen, wer die Vorratsdatenspeicherung anzuwenden hat. Ob die Liste öffentlich sein wird, ist nicht bekannt.

Gemäss Botschaft wird davon ausgegangen, dass anstatt 50 Access Provider neu bis zu 200 Firmen/Organisationen davon betroffen sein werden. Anders als der Bundesrat schreibt, geht es also sehr wohl um eine Ausweitung der Überwachung und nicht nur um eine Verbesserung.

Mit der Pflicht zur aktiven Überwachung müssen stets neue Einrichtungen auf eigene Kosten beschafft und unterhalten werden, was die betroffenen Unternehmen viele Hunderttausend Franken kostet und indirekt durch die Kunden bezahlt wird.

Die Überwachungsbehörden (der Dienst ÜPF) können zudem Qualitätskontrollen anordnen. Und für alle Betroffenen gilt: Bei Missachtung einer Verfügungen oder wenn eine Überwachung nicht geheim gehalten wird, können Bussen bis zu 100'000.- ausgesprochen werden, und es drohen Verurteilungen wegen Begünstigung. Die Überwachungsmachinerie hat also wie geölt zu funktionieren.

Aufgrund des Territorialitätsprinzips kann das Gesetz allerdings genau jene ausländische Anbieterinnen nicht umfassen, die heute diese Märkte dominieren und den grössten Teil der entsprechenden Kommunikation übermitteln (wie GMX, Skype, Whatsapp oder iMessage). Damit ist die massive Ausdehnung des Geltungsbereichs schlicht unnütz.

4 Schlussbemerkung / Forderung

Leider gibt es in der Schweiz keine Instanz, die Gesetze verbindlich an den Grund- und Menschenrechten misst. Solange der Gesetzgeber von den Strafverfolgungsbehörden getrieben scheint, bleiben diese jedoch wenig beachtet.

Im vorliegenden Entwurf geht es noch immer darum, den Strafverfolgungsbehörden möglichst weitreichende (teilweise auch bereits heute ohne genügende Rechtsgrundlagen praktizierte) Ermittlungsmöglichkeiten (Zwangsmassnahmen) an die Hand zu geben. Diese empirisch auf ihre Verhältnismässigkeit und auf eine Vereinbarkeit mit Grund- und Menschenrechten zu prüfen, wäre in den fast drei Jahren, seit Beginn der Vernehmlassung, angezeigt gewesen. Die dürftigen Ausführungen der Botschaft genügen diesen Anforderungen bei weitem nicht. Bevor die Verhältnismässigkeit nicht nachgewiesen ist, dürfen die Befugnisse aber nicht weiter ausgebaut und der Geltungsbereich nicht erweitert werden.

Die Digitale Gesellschaft lehnt den Entwurf daher als Ganzes ab.