Anträge der Digitalen Gesellschaft Schweiz betreffend BÜPF Revision (Geschäft 13.025)

Die Digitale Gesellschaft Schweiz zeigt auf den folgenden Seiten auf, wie die BÜPF-Revision entscheidend verbessert werden kann.

Bundesrat und Verwaltung möchten das Gesetz in der jetzigen Form verabschieden. Die Digitale Gesellschaft Schweiz hat bereits 2013 in einer Stellungnahme auf die Grundrechtsverletzungen und mangelnde Verhältnismässigkeit hingewiesen.

Sollten Sie Fragen zu einzelnen Anträgen haben oder ein persönliches Gespräch suchen, können Sie sich gerne melden.

Simon Gantenbein
simon.gantenbein@digitale-gesellschaft.ch

Anträge der Digitalen Gesellschaft Schweiz betreffend BÜPF Revision (Geschäft 13.025)

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 2 Persönlicher Geltungsbereich Aus diesem Gesetz ergeben sich Mitwirkungspflichten für die folgenden Personen (Mitwirkungspflichtige): a. Anbieterinnen von Postdiensten nach dem PG[4] b. Anbieterinnen von Fernmeldediensten nach Artikel 3 Buchstabe b des FMG c. Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste) d. Betreiberinnen von internen Fernmeldenetzen; e. Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen f. professionelle Wiederverkäuferinnen von Karten und ähnlichen Mitteln, die den Zugang zu einem öffentlichen Fernmeldenetz ermöglichen.	= Fassung Bundesrat	c. Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste) **mit grosser wirtschaftlicher Bedeutung und einer grossen Benutzerzahl** [...] e. Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz **als kommerzielles Angebot** Dritten zur Verfügung stellen	Art. 2 [b] 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. Art. 2 [c] Mit dieser Ausweitung des Geltungsbereichs auf sogenannte „Anbieterinnen abgeleiteter Kommunikationsdienste“ sollen sich Tausende kleine Anbieterinnen von Internetdiensten, die auch nur einen Mailserver für ein paar Freunde oder der ein Forum für den lokalen Tischtennisverein betreiben, zum verlängerten Arm der Strafverfolgungsbehörden machen. 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**. Art. 2[e] Neu fallen auch Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen unter die Mitwirkungspflicht. Dies sind insbesondere Hotels, Spitäler, Schulen, Bibliotheken oder ein WLAN-Zugang in einer Wohngemeinschaft. Von dem Geltungsbereich auszunehmen sind: • Privatpersonen und nicht-kommerzielle Vereine • Hotels, Spitäler, Schulen, Bibliotheken, Internet-Cafés Mehr Details finden Sie in der ausführliche Stellungnahme der Digitalen Gesellschaft unter http://www.digitale-gesellschaft.ch/buepf.pdf

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 10 Akteneinsichtsrecht 3 Die von einer Überwachung betroffene Person [...] Der Dienst ist nicht zuständig für die Auskunftserteilung. 4 Der Bundesrat regelt, auf welche Art diese Rechte gewährt werden. Dabei garantiert er die Parteirechte insbesondere in den Fällen, in denen die Anfertigung von Kopien der Akten unmöglich oder nur mit einem unverhältnismässigen Aufwand möglich ist.	= Fassung Bundesrat	(steichen) 3 Die von einer Überwachung betroffene Person [...] Der Dienst ist ~~**nicht**~~ zuständig für die Auskunftserteilung. 4 Der Bundesrat regelt, auf welche Art diese Rechte gewährt werden. Dabei garantiert er die Parteirechte insbesondere in den Fällen, in denen die Anfertigung von Kopien der Akten unmöglich ~~**oder nur mit einem unverhältnismässigen Aufwand möglich**~~ **ist.**	3 Der Dienst ÜPF verarbeitet Daten und ist Inhaber einer Datensammlung, somit sollte er gemäss DSG auch Auskünfte erteilen. Auch administrativ können die Prozesse so vereinheitlicht und die Qualität der Auskünfte gesteigert werden. 4 Der Dienst ÜPF muss die Daten so aufbewahren, dass beim Suchen kein unverhältnismässiger Aufwand entstehen kann.
Art. 11 Aufbewahrungsfrist für die Daten Die im Rahmen des Vollzugs eines Rechtshilfe-ersuchens gesammelten Daten sind im Verarbeitungssystem so lange aufzubewahren, wie es für das verfolgte Ziel erforderlich ist, längstens aber bis 30 Jahren nach Abschluss der Überwachung	= Fassung Bundesrat	[...] längstens aber bis **10 Jahre** nach Abschluss der Überwachung	Die übliche Verjährungsfrist von 10 Jahren reicht für die Verfahrensführung komplett aus.
Art. 11 Aufbewahrungsfrist für die Daten 7(neu)	= Fassung Bundesrat	7 (neu) **Daten, die nach Ablauf der Aufbewahrungsfirst in ein neues System überführt werden, benötigen zuvor eine richterliche Anordnung. Die Betroffenen müssen über die Fristverlängerung informiert werden.**	Es muss sichergestellt werden, dass die Aufbewahrungsfirst nicht umgangen werden kann. Ein Beispiel für einen Missbrauch im NDB (siehe [1]GPK Jahresbericht 2013, Punkt 4.2.3)

[1] http://www.parlament.ch/d/dokumentation/berichte/berichte-aufsichtskommissionen/geschaeftspruefungskommission-GPK/berichte-2014/Documents/jahresbericht-gpk-2013-d.pdf

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 12 Sicherheit 1 Der Dienst ist für die Sicherheit des Verarbeitungssystems verantwortlich.	= Fassung Bundesrat	(ergänzend) **Erkennt der Dienst Sicherheitslücken, oder werden solche an den Dienst herangetragen, so hat der Dienst Bundesrat und Öffentlichkeit zu informieren.** **Bei erheblichen Sicherheitslücken hat der Bundesrat den Betrieb der betroffenen Anwendung bis zur Behebung der Sicherheitslücken auszusetzen.** **Die Einstufung und Behebung der Schicherheitslücke wird durch eine unabhängige Partei begutachtet.**	Bei erheblichen Sicherheitslücken in Systemen welche für die Überwachung genutzt werden, soll der Bundesrat den Betrieb des Systems einstellen, bis die Sicherheitslücken behoben sind. Zudem ist die Öffentlichkeit zu informieren.
Art.16 Allgemeine Aufgaben bei der Überwachung (neu, Präzisierung)	k. Er führt eine Statistik über die Überwachungen	**k. Er veröffentlicht jährlich eine Statistik über die Überwachungen nach Aufträgen. Insbesondere müssen Delikt, Kanton, Überwachungstyp, Art der Überwachung und die Kosten von Einkauf und Betrieb des Auftrages ausgewiesen werden.** **l. Alle zwei Jahre legt der Dienst eine unabhängige Wirksamkeitsanalyse nach Art der Überwachung und Delikt vor.** **m. Der Dienst veröffentlicht jährlich eine Statistik über den Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs nach StPO 269ter. Insbesondere müssen Art, Dauer und Kosten ausgewiesen werden.** **n. Verfügen kantonale Strafverfolgungs-behörden selber über solch besondere Informatikprogramme so ist dies gegenüber dem Dienst auszuweisen und in die Statistik aufzunehmen.**	Der Dienst ÜPF veröffentlicht bereits heute eine detaillierte Statistik in Excel. Neu sollen zusätzlich die Kosten eines Auftrages ausgewiesen werden. Eine periodische Überprüfung der Wirksamkeit von Überwachungsmassnahmen fehlt im Gesetzesentwurf. Nach dem Gesetzesvorschlag muss über den Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs nach StPO 269ter (IMSI-Catchern) keine Statistik geführt werden. Derzeit sind die Massnahmen kantonaler Strafver-folgungsbehörden nicht von der Statistik erfasst.

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 22 Auskünfte zur Identifikation [4] Der Bundesrat kann Anbieterinnen abgeleiteter Kommunikationsdienste, die Dienstleistungen von grosser wirtschaftlicher Bedeutung **oder** für eine grosse Benutzerschaft anbieten, verpflichten, alle oder einen Teil der Angaben bereit zu halten und zu liefern, welche die Anbieterinnen von Fernmeldediensten gestützt auf Absatz 2 liefern müssen.	= Fassung Bundesrat	[4] Der Bundesrat kann Anbieterinnen abgeleiteter Kommunikationsdienste, die Dienstleistungen von grosser wirtschaftlicher Bedeutung ~~**oder**~~ **und** für eine grosse Benutzerschaft anbieten, verpflichten [...]	Kleinere Unternehmen, Organisationen und Vereine sollen vor der Investition in Überwachungstechnik geschützt werden. Diese sind, das zeigen auch Statistiken, für die Strafverfolgung nicht relevant.
Art. 22 Auskünfte zur Identifikation [5] (neu)		(neu) Betreffen die Auskünfte Randdaten, die aufgrund Art. 26 Abs. 5 vorgehalten werden, müssen die Voraussetzungen nach Art. 273 StPO erfüllt sein.	Der Bunderatsentwurf lässt eine Auskunft zur Identifikation ohne Einschränkung zu. Statt eines Deliktskatalogs sollen Straftaten die mit Freiheitsstrafe nicht unter einem Jahr bedroht sind, regeln, wann eine Identifikation zulässig ist. Betreffen die Auskünfte Daten aus der Vorratsdaten-speicherung, soll kein vereinfachtes Verfahren und kein unbeschränkter Deliktskatalog gelten.
Art. 25 Informationen über Dienstleistungen Die Anbieterinnen von Fernmeldediensten informieren den Dienst auf Verlangen jederzeit ausführlich über Art und Merkmale der Dienstleistungen, die sie auf den Markt gebracht haben oder innerhalb von sechs Monaten auf den Markt bringen wollen.	= Fassung Bundesrat	(streichen) Die Anbieterinnen von Fernmeldediensten informieren den Dienst auf Verlangen jederzeit ausführlich über Art und Merkmale der Dienstleistungen, die sie auf den Markt gebracht haben ~~**oder innerhalb von sechs Monaten auf den Markt bringen wollen.**~~	Die Anbeiterinnen müssen laut dem Entwurf den Dienst ÜPF informieren, welche Produkte sie gedenken auf den Markt zu bringen. Die Absicht des Dienstes ist es, sich so gut wie möglich auf Neuerungen im Internet zu reagieren. Aber mit diesem Artikel müssen die Anbieterinnen unter umständen Geschäftsgeheimnisse preisgeben. Es ist zu befürchten, dass Innovationen gehemmt werden können. Daher soll die Informationspflicht nur für existierende, aber nicht zukünftige Dienstleistungen gelten.

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 26 Pflichten der Anbieterinnen von Fernmeldediensten [1] Anbieterinnen von Fernmeldediensten liefern dem Dienst oder nach Artikel 17 Buchstabe c der anordnenden Behörde oder der von dieser bezeichneten Behörde auf Verlangen:		(ergänzend) [1] **Bezieht die überwachte Person bei der Anbieterin einen überwachten Fernmeldedienst, liefert die Anbieterin des Fernmeldedienstes** ~~**Anbieterinnen von Fernmeldediensten liefern**~~ dem Dienst oder nach Artikel 17 Buchstabe c der anordnenden Behörde oder der von dieser bezeichneten Behörde **soweit vorhanden oder mit verhältnis-mässigem Aufwand möglich** auf Verlangen:	
[2] Sie müssen zudem: c. von ihnen angebrachte Verschlüsselungen entfernen.	= Fassung Bundesrat	(ergänzend) Art. 26 [2] c von ihnen angebrachte Verschlüsselungen entfernen, **soweit dies technisch möglich ist.**	Es gibt Systeme, die so konstruiert sind, dass sogar die Anbieterin den Inhalt der Kommunikation nicht auslesen kann. Bei solchen Systemen kann die angebrachte Verschlüsselung nicht entfernt werden.

Vorratsdatenspeicherung

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 26 Pflichten der Anbieterinnen von Fernmeldediensten Ziffer 5 (Randdaten) Die Anbieterinnen von Fernmeldediensten müssen die Randdaten des Fernmeldeverkehrs während 12 Monaten aufbewahren.	= Fassung Bundesrat Minderheit (Stadler Markus, Minder, Schmid Martin) .. während 8 Monaten aufbewahren	Die Anbieterinnen von Fernmeldediensten müssen die Randdaten des Fernmeldeverkehrs **~~während 12 Monaten~~ auf Antrag der Ermittlungs- oder Untersuchungsbehörde aufbewahren (Quick Freeze).** **Den Zugriff regelt Art. 273 StPO.** **Die Digitale Gesellschaft Schweiz empfiehlt dringend einen Richtungswechsel zum Quick-Freeze-Verfahren.**	Eine präventive Überwachung sämtlicher BewohnerInnen - durch Erhebung und Speicherung der Kommunikations- und Lokationsdaten für 6 oder 12 Monate - ist mit einem Rechtsstaat nicht zu vereinen. Eine Studie des renommierten Max-Planck-Institut im Auftrag des deutschen Bundesamtes für Justiz kommt zudem 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. Der Europäische Gerichtshof (EuGH) hat im April 2014 entschieden, dass die Richtlinie zur Vorratsdaten-speicherung in Europa ausgesetzt werden muss. Es ist fahrlässig, diesen Gesetzes-vorschlag im Kontext des EuGH-Urteils zu verabschieden. Mit dem Quick-Freeze-Verfahren[2] kann auf eine Vorratsdatenspeicherung verzichtet werden, da nur Personen erfasst werden, die in eine Untersuchung involviert sind und nicht jedermann. Die Digitale Gesellschaft hat im Februar beim Dienst ÜPF ein Gesuch auf Unterlassung der Vorratsdatenspeicherung[3] eingereicht. Die Beschwerde wird nötigenfalls bis zum Europäischen Gerichtshof für Menschenrechte

2 Quick Freeze Verfahren: https://de.wikipedia.org/wiki/Quick_Freeze
3 Gesuch auf Unterlassung der Vorratsdatenspeicherung http://digiges.ch/Beschwerde_20140220.pdf

			weitergezogen.

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 26 Pflichten der Anbieterinnen von Fernmeldediensten Ziffer 6 Der Bundesrat kann Anbieterinnen von Fernmeldediensten von bestimmten gesetzlichen Pflichten befreien, insbesondere wenn sie Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Bildungsbereich anbieten. Er befreit sie nicht von der Pflicht, die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person auf Verlangen zu liefern sowie von den Pflichten nach Absatz 2.	= Fassung Bundesrat	Der Bundesrat **~~kann~~ befreit** Anbieterinnen von Fernmeldediensten von bestimmten gesetzlichen Pflichten **~~befreien~~**, insbesondere wenn sie Dienstleistungen von geringer **wirtschaftlicher Bedeutung für die Aufklärung strafbarer Handlungen** oder im Bildungsbereich anbieten. **~~Er befreit sie nicht von der~~ Ausgenommen bleibt die** Pflicht, die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person auf Verlangen zu liefern **~~sowie von den Pflichten nach Absatz 2.~~**	Siehe Bemerkungen Art. 2 Geltungsbereich
Art. 26 (ergänzend) Rasterfahndung		(ergänzend) Die Randaten dürfen nicht zur Rasterfahndung (Antennensuchlauf) verwendet werden.	Diese Ergänzung stellt sicher, dass die erhobenen Randdaten nicht zur Rasterfahndung verwendet werden.

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 27 Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste [1] Anbieterinnen abgeleiteter Kommunikationsdienste müssen eine Überwachung betreffend der Daten, welche die überwachte Person unter Verwendung abgeleiteter Kommunikationsdienste übermittelt oder speichert, durch den Dienst oder durch die von diesem beauftragten Personen dulden.	= Fassung Bundesrat	[1] Anbieterinnen abgeleiteter Kommunikationsdienste müssen ~~eine Überwachung betreffend der Daten, welche die überwachte Person unter Verwendung abgeleiteter Kommunikationsdienste übermittelt oder~~ **speichert, durch den Dienst oder durch die von diesem beauftragten Personen dulden. Zu diesem Zweck müssen sie unverzüglich: a. Zugang zu ihren Anlagen gewähren; b. die für die Überwachung notwendigen Auskünfte erteilen.**	Eine Einschränkung auf eine Auskunftspflicht betreffend der bereits vorhandenen Randdaten. Das „Dulden“ von darüber hinausgehender, aktiver Überwachung würden bedeuten, kurzfristig und ohne sorgfältige Tests oder Sicherheitsanalyse Änderungen um laufenden System vorzunehmen, die darum die Sicherheit und die Stabilität des angebotenen abgeleiteten Kommuniationsdienstes gefährden. Die Schweiz darf nicht als Standort für die Erbringung von geschäftskritischen Dienstleistungen ungeeignet gemacht werden!
Zu diesem Zweck müsssen sie unverzüglich: a. Zugang zu ihren Anlagen gewähren; b. die für die Überwachung notwendigen Auskünfte erteilen.		[2] **Sie müsse**~~n~~ auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern.	Es sollen nur Unternehmen für eine Auskunft herbeigezogen werden können, die eine wirtschaftliche Bedeutung haben und zugleich viele User haben.
[3] Soweit für die Überwachung des Fernmeldeverkehrs notwendig, unterstellt der Bundesrat alle oder einen Teil der Anbieterinnen abgeleiteter Kommunikationsdienste, die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten, allen oder einem Teil der in Artikel 26 genannten Pflichten. Für die Anbieterinnen von Fernmeldediensten geltende Bestimmungen dieses Gesetzes sind diesfalls sinngemäss anwendbar.		[2 3] ~~**Soweit für die Überwachung des Fernmeldeverkehrs notwendig, unterstellt**~~ der Bundesrat **kann** alle oder einen Teil der Anbieterinnen abgeleiteter Kommunikationsdienste, die Dienstleistungen von grosser wirtschaftlicher Bedeutung ~~**oder**~~ **und** für eine grosse Benutzerschaft anbieten, allen oder einem Teil der in Artikel 26 genannten Pflichten **unterstellen**. Für die Anbieterinnen von Fernmeldediensten geltende Bestimmungen dieses Gesetzes sind diesfalls sinngemäss anwendbar.	Von den Pflichten auszunehmen sind: • Privatpersonen und nicht-kommerzielle Vereine • Hotels, Spitäler, Schulen, Bibliotheken, Internet-Cafés Siehe Bemerkungen Art. 2 Geltungsbereich

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 28 Pflichten der Betreiberinnen von internen Fernmeldenetzen 1 Betreiberinnen von internen Fernmeldenetzen müssen eine Überwachung durch den Dienst oder durch die von diesem beauftragten Personen dulden. Zu diesem Zweck müssen sie unverzüglich: a. Zugang zu ihren Anlagen gewähren; b. die für die Überwachung notwendigen Auskünfte erteilen. 2 Sie müssen auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern.	= Fassung Bundesrat	1 Betreiberinnen von internen Fernmeldenetzen **müssen** ~~**eine Überwachung durch den Dienst oder durch die von diesem beauftragten Personen dulden. Zu diesem Zweck müssen sie unverzüglich:** ~~**a. Zugang zu ihren Anlagen gewähren;** ~~**b. die für die Überwachung notwendigen Auskünfte erteilen.**~~ 2 ~~**Sie müssen**~~ auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern.	Siehe Bemerkungen Art. 2 Geltungsbereich Vertrauenspersonen wie Lebenspartner, WG-Mitbewohner, Familienangehörige oder Klassenlehrer müssten eine Überwachung dulden. Diese existenziellen Gewissenskonflikte können für Pflichtige untragbar sein und grenzen an Erpressung wenn man die Bussen Art. 39d beachtet.
Art. 29 Pflichten der Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen 1 Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen, müssen eine Überwachung durch den Dienst oder durch die von diesem beauftragten Personen dulden. Zu diesem Zweck müssen sie unverzüglich: a. Zugang zu ihren Anlagen gewähren; b. die für die Überwachung notwendigen Auskünfte erteilen. 2 Sie müssen auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern.	= Fassung Bundesrat	1 Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen, ~~**müssen eine Überwachung durch den Dienst oder durch die von diesem beauftragten Personen dulden. Zu diesem Zweck müssen sie unverzüglich:** ~~**a. Zugang zu ihren Anlagen gewähren;** ~~**b. die für die Überwachung notwendigen Auskünfte erteilen.**~~ 2 ~~**Sie**~~ müssen auf Verlangen die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs der überwachten Person liefern.	

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 32 Auskunfts- und Überwachungsbereitschaft [1] Die Anbieterinnen von Fernmeldediensten müssen jederzeit in der Lage sein, gemäss dem anwendbaren Recht die Auskünfte nach den Artikeln 21 und 22 und die Informationen nach den Artikeln 24 und 26 Absatz 2 Buchstabe a zu erteilen und die von ihnen angebotenen Fernmeldedienste zu überwachen, wenn die Auskunftserteilung beziehungsweise Überwachung standardisiert ist. [2] Werden Auskünfte verlangt oder Überwachungstypen angeordnet, die nicht standardisiert sind, so müssen die Anbieterinnen von Fernmeldediensten entsprechend den Anweisungen des Dienstes mit diesem zusammenarbeiten und alle geeigneten Massnahmen treffen, um die reibungslose Umsetzung sicherzustellen.		[1] Die Anbieterinnen von Fernmeldediensten müssen **~~jederzeit~~** in der Lage sein, gemäss dem anwendbaren Recht die Auskünfte nach den Artikeln 21 und 22 und die Informationen nach den Artikeln 24 und 26 Absatz 2 Buchstabe a zu erteilen und die von ihnen angebotenen Fernmeldedienste zu überwachen, wenn die Auskunftserteilung beziehungsweise Überwachung standardisiert ist. [2] Werden Auskünfte verlangt oder Überwachungstypen angeordnet, die nicht standardisiert sind, so müssen die Anbieterinnen von Fernmeldediensten entsprechend den Anweisungen des Dienstes mit diesem zusammenarbeiten und alle geeigneten **und in technischer und finanzieller Hinsicht verhältnismässigen** Massnahmen treffen, um die reibungslose Umsetzung sicherzustellen.	Verhältnismässigkeit bleibt gewahrt.
Art. 33 Nachweis der Auskunfts- und Überwachungsbereitschaft [1] Auf Verlangen des Dienstes müssen die Anbieterinnen von Fernmeldediensten auf eigene Kosten nachweisen, dass sie in der Lage sind, gemäss dem anwendbaren Recht die standardisierten Auskünfte zu erteilen und die standardisierten Überwachungen durchzuführen.	= Fassung Bundesrat	(streichen) **~~[1] Auf Verlangen des Dienstes müssen die Anbieterinnen von Fernmeldediensten auf eigene Kosten nachweisen, dass sie in der Lage sind, gemäss dem anwendbaren Recht die standardisierten Auskünfte zu erteilen und die standardisierten Überwachungen durchzuführen.~~**	Ziffer 1 streichen

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 41 Aufsicht (neu)		(neu) **Der Bundesrat sorgt dafür, dass die Tätigkeit des Dienstes auf Zweckmässigkeit und Wirksamkeit überprüft wird und erstattet regelmässig Bericht.**	Im Bericht [4] der UN Hochkommissarin für Menschenrechte, ist das Belegen der Wirksamkeit von Überwachungsmassnahmen eine Voraussetzung für die Vereinbarkeit mit dem internationalen Menschenrechts-Recht: *The very existence of a mass surveillance Programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful.* Bei Massnahmen bei denen die Wirksamkeit für legitime Zwecke der Verbrechensbekämpfung nicht belegt werden, handelt es sich um „arbitrary iterference“.
Art. 42 Rechtsschutz […] [2] Mit Beschwerde gegen die Verfügungen des Dienstes kann nicht geltend gemacht werden, die Voraussetzungen für die Anordnung der Überwachung seien nicht erfüllt. [3] Die Beschwerde hat keine aufschiebende Wirkung, ausser wenn die Verfügung eine Geldleistung betrifft. Die Beschwerdeinstanz kann der Beschwerde aufschiebende Wirkung verleihen.	= Fassung Bundesrat RK-S: [2] streichen	(Ziffer 2 und 3 streichen) […] [2] **~~Mit Beschwerde gegen die Verfügungen des Dienstes kann nicht geltend gemacht werden, die Voraussetzungen für die Anordnung der Überwachung seien nicht erfüllt.~~** [3] **~~Die Beschwerde hat keine aufschiebende Wirkung, ausser wenn die Verfügung eine Geldleistung betrifft. Die Beschwerdeinstanz kann der Beschwerde aufschiebende Wirkung verleihen~~**.	Es muss möglich sein, gegen eine Anordnung des Dienstes Beschwerde zu führen. Dies geschieht nach dem die Überwachungsmassnahme abgeschlossen ist und behindert die Strafverfolgung nicht.

4 Bericht des UN Hochkommissariats für Menschenrecht, siehe Absatz 20 http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

IMSI Catcher

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 269bis Einsatz von besonderen technischen Geräten zur Überwachung des Fernmeldeverkehrs [1] Die Staatsanwaltschaft kann den Einsatz besonderer technischer Geräte zur Überwachung des Fernmeldeverkehrs anordnen, um Gespräche mitzuhören oder aufzunehmen oder eine Person oder Sache zu identifizieren oder deren Standort zu ermitteln, wenn: a. die Voraussetzungen von Artikel 269 erfüllt sind; b. die bisherigen Massnahmen zur Überwachung des Fernmeldeverkehrs nach Artikel 269 erfolglos geblieben sind oder die Überwachung mit diesen Massnahmen aussichtlos wäre oder unverhältnismässig erschwert würde; c. die für den Einsatz dieser Geräte aufgrund des Fernmelderechts nötigen Bewilligungen zum Zeitpunkt des Einsatzes vorliegen.	= Fassung Bundesrat	**Streichung Art. 269bis** (bei Nicht-Streichung) **Sämtliche erfassten Personen müssen nach Abschluss des Ermittlungs-verfahrens benachrichtigt werden.**	Laut Botschaft geht es namentlich um den Einsatz von Überwachungsgeräten wie IMSI-Catchern. Ein IMSI-Catcher schiebt sich im Handynetz zwischen die Mobiltelefone in der Umgebung und das eigentliche Mobilfunknetz. Er ermöglicht die sofortige Identifizierung der Netzteilnehmer, die Erstellung eines Bewegungsprofils und das Mithören von Handyanrufen. **Der Einsatz solcher Geräte ist nicht grundrechtsverträglich**. Klar wird dies, wenn man sich eine gesetzliche Norm vorstellt, die es der Polizei erlauben würde, auf einen Schlag die Identität aller Personen, die sich in einem bestimmten Gebiet aufhalten, zu kontrollieren und alle Namen zu protokollieren. Nachdem heute fast jede Person ein Handy auf sich trägt, läuft der Einsatz des IMSI-Catchers auf eine solche flächendeckende Personenkontrolle in einem bestimmten Umkreis hinaus – ohne dass es die Betroffenen merken. Ein weiterer Aspekt sind unbeteiligte Dritte, die einen Notruf tätigen wollen und sich mit dem IMSI-Catcher verbinden. Diese Notrufe können nicht garantiert zu der Notrufzentrale verbunden werden. Dies widerspricht dem Artikel 16 des Fernemdegesetztes (FMG) und beschneidet den Umfang der Grundversorgung in der "den Zugang zu Notrufdiensten“ gewährt werden soll.

GovWare / Staatstrojaner

Die Digitale Gesellschaft Schweiz empfiehlt auf GovWare komplett zu verzichten!
Vorab stellt sich die Frage der Verhältnismässigkeit. Der Einsatz beschneidet zum einen die Grundrechte, zum Anderen zeichnen sich technische Probleme und und ausufernd Kosten ab. Der Deutsche Bundestrojaner kostet jährlich über 1 Mio. €. Die Strafuntersuchungsbehörden rechnen mit einigen wenigen Fällen (etwa 10) pro Jahr. GovWare ist teuer und die Kosten sind wegen Weiterentwicklungen wiederkehrend. Mehr Details finden Sie in der ausführliche Stellungnahme unter www.digitale-gesellschaft.ch/buepf.pdf

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
StPO Art. 269ter Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs [1] Die Staatsanwaltschaft kann das Einschleusen von besonderen Informatik-programmen in ein Datenverarbeitungssystem anordnen, um den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs in unverschlüsselter Form abzufangen und auszuleiten, wenn: a. die Bedingungen von Artikel 269 Absatz 1 und 3 erfüllt sind; b. es sich um eine Strafverfolgung nach Artikel 286 Absatz 2 handelt; c. die bisherigen Massnahmen zur Überwachung des Fernmeldeverkehrs nach Artikel 269 erfolglos geblieben sind oder die Überwachung mit diesen Massnahmen aussichtlos wäre oder unverhältnismässig erschwert würde. [2] Die Staatsanwaltschaft bezeichnet in der Überwachungsanordnung a. die gewünschten Datentypen; und b. die nicht öffentlichen Räume, in die allenfalls eingedrungen werden muss, um besondere Informatikprogramme in das betreffende Datenverarbeitungssystem einzuschleusen.	= Fassung Bundesrat	[1] Die Staatsanwaltschaft kann das Einschleusen von besonderen Informatik-programmen in ein Datenverarbeitungs-system anordnen, um den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs in unverschlüsselter Form abzufangen und auszuleiten, wenn: a. die Bedingungen von Artikel 269 Absatz 1 und 3 erfüllt sind; b. es sich um eine Strafverfolgung ~~**nach Artikel 286 Absatz 2**~~ **eines Verbrechens oder Vergehens handelt, das mit Freiheitsstrafe nicht unter einem Jahr bedroht ist;** c. die bisherigen Massnahmen zur Überwachung des Fernmeldeverkehrs nach Artikel 269 erfolglos geblieben sind oder die Überwachung mit diesen Massnahmen aussichtlos wäre oder unverhältnismässig erschwert würde. [2] Die Staatsanwaltschaft bezeichnet in der Überwachungsanordnung a. die gewünschten Datentypen; und b. die nicht öffentlichen Räume, in die allenfalls eingedrungen werden muss, um besondere Informatikprogramme in das betreffende Datenverarbeitungssystem einzuschleusen. *Fortsetzung nächste Seite*	Im Deliktekatalog finden sich auch Straftatbestände wie z.B. Diebstahl (Art. 139 StGB). Somit könnte zukünftig bei einem leichten Diebstahl ein Trojaner bewilligt werden. Anstatt eines eines Deliktekatalogs sollten nur schwere Delikte die mit Freiheitsstrafe nicht unter einem Jahr bedroht sind für Staatstrojaner zugelassen werden. Verwendet man statt eines Deliktekatalogs die schwere der Straftat, so kann ein schwerer Diebstahl geahndet werden, da dieser mit bis zu fünf Jahren Freiheitsstrafe bestraft werden kann. Wird dieses Prinzip eingeführt, gibt es klare Masstäbe und nicht einen schwammigen Deliktskatalog.

Botschaft Bundesrat	Ständerat	Antrag Digitale Gesellschaft	Bemerkungen
Art. 269ter Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs [3] Durch Absatz 1 nicht gedeckte Daten, die beim Einsatz solcher Informatikprogramme gesammelt werden, sind sofort zu vernichten. Durch solche Daten erlangte Erkenntnisse dürfen nicht verwertet werden.	= Fassung Bundesrat	[3] Durch Absatz 1 nicht gedeckte Daten **dürfen durch solche ~~die beim Einsatz solcher~~** Informatikprogramme **nicht** gesammelt werden **~~, sind sofort zu vernichten. Durch solche Daten erlangte Erkenntnisse dürfen nicht verwertet werden.~~** (neu ff.) **[4] Für die Strafuntersuchung nicht relevante Daten aus der Überwachung, namentlich die Intim- und Privatsphäre betreffend, sind umgehend zu löschen.** **[5] Für das Einschleusen von besonderen Informatikprogrammen dürfen keine Sicherheitslücken aus dem Grau- oder Schwarzmarkt verwendet werden.** **[6] Die Sicherheit des betroffenen Datenverarbeitungssystems darf durch die Massnahme in keiner Weise beeinträchtigt werden.** **[7] Nach Abschluss der Massnahme muss das Datenverarbeitungssystem in seinen Ursprungszustand versetzt werden.** **[8] Unrechtmässig erlangte Daten und Erkenntnisse dürfen nicht verwendet werden.**	Verbesserung der Grundrechte: Technische Beschränkung der Überwachung auf Daten aus einem laufenden Telekommunikationsvorgang Unmittelbare Löschung nicht relevanter oder zulässiger Daten aus der Überwachung z.B. Ausschalten des Antivirenscanners