Zusammenfassung der eingereichten Stellungnahme

Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit

Eröffnung	27.05.2026
Eingabefrist	17.09.2026
Zuständiges Departement	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK)
Zuständige Bundesstelle	Bundesamt für Kommunikation (BAKOM)
Zuständige Organisation	Telecomrecht
Adresse	Zukunftstrasse 44, 2500, Biel/Bienne
Unterlagen und Informationen	https://fedlex.data.admin.ch/eli/dl/proj/2026/38/cons_1
Kontaktperson	Joëlle Pizarro (tp-secretariat@bakom.admin.ch) , Stéphane Bondallaz (tp-secretariat@bakom.admin.ch)
Telefon	+41 58 46 05876

Kontaktangaben zur Stellungnahme

Name der Person oder Organisation	Piratenpartei Schweiz (PPS)
Zuständige Stelle	Vorstand
Adresse	3000 Bern
Vorname	Renato
Nachname	Sigg
Telefonnummer für Rückfragen	--
Einreichungsdatum	17.09.2026

Rückmeldung zu: Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit: Fernmeldegesetz (FMG)

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Eher Ablehnung
Begründung	Die Piratenpartei Schweiz begrüsst grundsätzlich die Verstärkung der technischen Sicherheit und Resilienz der Schweizer Fernmeldeinfrastruktur. Vor allem die Pflicht zu sicheren Systemkonfigurationen, der Rückbau kritischer Abhängigkeiten, die Verbesserung der Notkommunikation sowie die Angleichung des Fernmelderechts an moderne, softwarebasierte Infrastrukturen sind grundsätzlich verständlich. Die Vorlage vermengt jedoch mehrere stark voneinander abweichende Regelungsbereiche. Ausserhalb der klassischen Netz- und Infrastruktursicherheit enthält sie neue Instrumente im Bereich der Betrugsbekämpfung, des Jugendschutzes, der Datenbearbeitung, der Überwachung beziehungsweise automatisierten Erfassung sowie der polizeinahen Gefahrenabwehr. Teils wird dabei der Fernmeldebereich als Ausgangspunkt für Massnahmen genutzt, deren eigentliche Zielsetzung über die Regulierung der technischen Telekommunikationsinfrastruktur weit hinausgeht. Vier Entwicklungen bewerten wir als besonders problematisch: Erstens verlagern sich Entscheidungen über gravierende Eingriffe zunehmend von Gerichten oder regulären Strafverfolgungsbehörden auf Verwaltungsorgane und private Fernmeldedienstanbieterinnen. Dies betrifft vor allem die Sperrung von Telefonnummern und Domain-Namen. Gerade Eingriffe in Kommunikationsmöglichkeiten dürfen nicht ausschliesslich auf Basis eines administrativ festgestellten Verdachts erfolgen, wenn eine unabhängige richterliche Kontrolle machbar und zumutbar ist. Umso problematischer ist, dass der erläuternde Bericht bei diesen Sperrinstrumenten selbst erhebliche verfassungsrechtliche Unsicherheiten festhält. Er bezeichnet die Sperrung nach Art. 6b ausdrücklich als Einschränkung der Kommunikationsfreiheit und bei kommerzieller Nutzung auch der Wirtschaftsfreiheit. Gleichzeitig hält er fest, dass Zweifel bestehen, ob die Massnahmen nach Art. 6a und 6b auf Art. 92 BV gestützt werden können, und dass die geeignete verfassungsrechtliche Grundlage noch eingehend zu klären sei. Es erscheint uns rechtsstaatlich verkehrt, zunächst neue grundrechtsrelevante Sperrbefugnisse zu schaffen und erst anschliessend abschliessend zu klären, ob der Bund hierfür überhaupt über eine hinreichende verfassungsrechtliche Kompetenz verfügt. Zweitens schafft die Vorlage neue Grundlagen für Profiling inklusive der Bearbeitung besonders schützenswerter Personendaten. Besonders bedenklich ist, dass ausdrücklich biometrische Daten erwähnt werden und ein Profiling nötigenfalls ohne Kenntnis der betroffenen Personen erfolgen darf. Derartige Instrumente sieht die Vorlage sowohl im Bereich der Domain-Namen als auch zum Schutz der Fernmeldeinfrastrukturen vor. Die Rechtfertigung, dass diese Befugnisse voraussichtlich nur ausnahmsweise in Anspruch genommen würden, ersetzt keine möglichst enge gesetzliche Begrenzung und begründet bestenfalls deren Streichung. Die vorgesehenen Änderungen wirken auffällig häufig wie ein Ausbau der Überwachungsmöglichkeiten durch das Fernmeldegesetz. Drittens enthält die Vorlage zahlreiche Delegationen an den Bundesrat und an das BAKOM. Dort, wo Grundrechte berührt sind – namentlich bei Profiling, biometrischen Daten, Kommunikationssperren, automatisierter Erfassung und der Entfernung von Infrastruktur –, müssen die wesentlichen Voraussetzungen auf Gesetzesstufe festgelegt werden. Der erläuternde Bericht zählt selbst eine nicht geringe Zahl neuer oder erweiterter Rechtsetzungsdelegationen auf. Viertens erachten wir den Verzicht auf eine umfassende Datenschutz-Folgenabschätzung als nicht überzeugend. Der Bericht geht davon aus, dass besonders schützenswerte Personendaten und Profiling nur in Ausnahmefällen betroffen seien, weshalb vorerst keine weitergehende Datenschutz-Folgenabschätzung nötig sei. Gerade die gesetzliche Schaffung mehrerer neuer Bearbeitungsbefugnisse für biometrische Daten, Profiling und Verkehrsdaten rechtfertigt unseres Erachtens eine vertiefte Folgenabschätzung schon vor Erlass des Gesetzes.
Anhang	

Detaillierte Stellungnahme

Titel	Art. 1 Abs. 1 sowie 2 Bst b und f
Antwortoption	Zustimmung
Anpassungen / Gegenvorschlag	--
Begründung	Die Ergänzung des Gesetzeszwecks um die Sicherheit von Fernmeldediensten sowie um die Sicherheit und Resilienz der Fernmeldeinfrastruktur ist grundsätzlich sachlich angemessen. Cybersicherheit und Informationssicherheit sind zwingende Voraussetzungen für die Wahrung von Privatsphäre und informationeller Selbstbestimmung. Die Piratenpartei Schweiz befürwortet deshalb eine ausdrückliche Verankerung dieses Ziels. Entscheidend ist allerdings, dass der Sicherheitsbegriff nicht als generelle Rechtfertigung für die Überwachung von Kommunikationsinhalten ausgelegt werden darf. Positiv ist die Klarstellung im Erläuterungsbericht, dass Anbieterinnen keine Inhaltskontrolle vornehmen sollen und das Fernmeldegeheimnis weiterhin Bestand hat - noch besser wäre es erneut eindeutig im Gesetz verankert.
Anhang	

Titel	Art. 3a Rechte und Pflichten von Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen
Antwortoption	Neutrale Haltung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 3a sieht vor, dass auch blosse Anbieter für Dritte gewissen Regeln unterstellt sind, wie dies für direkte Anbieterinnen von Fernmeldediensten gilt. Absatz 2 ist allerdings kritisch zu sehen. Er erlaubt dem Bundesrat pauschal, weitere Rechte und Pflichten von Anbieterinnen sinngemäss auf Infrastruktureigentümerinnen und -betreiberinnen auszudehnen. Damit können Pflichten grundsätzlich auf eine neue Gruppe von Adressaten erstreckt werden. Eine offene Abtretung dieser Art ist bedenklich, wenn aus ihr erhebliche Datenbearbeitungspflichten hervorgehen könnten.
Anhang	

Titel	Art. 4 Registrierung
Antwortoption	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Es ist verständlich, dass das BAKOM für seine Aufsichtsaufgaben wissen muss, welche relevanten Unternehmen auf dem Schweizer Fernmeldemarkt aktiv sind. Der Begriff der «massgeblichen technischen oder wirtschaftlichen Bedeutung» in Artikel 4 Absatz 3 bleibt jedoch schwammig. Der Kreis potenziell registrierbarer Unternehmen sollte auf Gesetzesstufe anhand transparenter und objektiver Kriterien exakt umrissen werden. Eine Registrierung darf nicht in eine faktische allgemeine Registrierungspflicht für beliebige Internetdienste oder kleinere technische Anbieter entarten. Die zusätzlich erhobenen Daten sind gemäss dem Grundsatz der Datenminimierung auf das für Aufsicht und Statistik tatsächlich nötige Minimum zu beschränken.
Anhang	

Titel	Art. 4a Meldepflicht
Antwortoption	Neutrale Haltung
Anpassungen / Gegenvorschlag	--
Begründung	Eine Registrierung darf nicht in eine faktische allgemeine Registrierungspflicht für beliebige Internetdienste oder kleinere technische Anbieter entarten. Die zusätzlich erhobenen Daten sind gemäss dem Grundsatz der Datenminimierung auf das für Aufsicht und Statistik tatsächlich nötige Minimum zu beschränken.
Anhang	

Titel	Art. 6a Sperrung des Zugangs zu Telefonie und Internet
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	1 Die Anbieterinnen von Fernmeldediensten müssen den Zugang zu Telefonie und Internet für Personen sperren: a. die gegenüber der Anbieterin: 1. eine fiktive Identität verwendet haben, 2. die Identität einer Person verwendet haben, die mit der Anbieterin kein Vertragsverhältnis eingehen wollte; b. die sich gegenüber der Anbieterin mit einem Dokument ausgewiesen haben, das die Anforderungen nach dem Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) nicht erfüllt; c. wenn die Übermittlung des Dokuments an die zuständigen Behörden in der Schweiz, mit dem sich die Person gegenüber der Anbieterin im Ausland ausgewiesen hat, aus technischen oder juristischen Gründen nicht stattgefunden hat. -> Streichung 2 Die zuständigen Behörden stellen sicher, dass auf eine Sperrung verzichtet wird, wenn ihnen bekannt ist, dass der betreffende Zugang zu Internet oder Telefonie Gegenstand eines Überwachungsauftrags des Diensts Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ist. In diesen Fällen erfolgt eine Rücksprache mit dem Dienst ÜPF. -> Ersatzlos streichen im Übrigen Verhältnismässigkeit und Rechtsschutz explizit regeln ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt

Begründung	Artikel 6a sieht als einschneidende Rechtsfolge die vollständige Sperrung des Zugangs zu Telefonie und Internet vor. Der Internetzugang ist heute aber für gesellschaftliche, berufliche und wirtschaftliche Teilhabe unverzichtbar. Hinzu kommt, dass diese einschneidende Sperre unmittelbar durch die Fernmeldedienstanbieterin zu vollziehen ist, ohne dass der Artikel eine vorgängige unabhängige oder richterliche Prüfung vorsieht. Der erläuternde Bericht hält zudem fest, dass Zweifel bestehen, ob die Sperrmassnahme nach Art. 6a auf Art. 92 BV gestützt werden kann. Hinsichtlich der Massnahmen nach Art. 6a und 6b müsse die geeignete verfassungsrechtliche Grundlage noch eingehend geprüft und im Rahmen der Vorarbeiten zur Botschaft geklärt werden. (S. 78f. erläuternder Bericht) Besonders problematisch ist Absatz 1 Buchstabe c. Gemäss dieser Bestimmung soll eine Sperrung vorgenommen werden, wenn die Übermittlung eines im Ausland zur Identifikation genutzten Dokuments an die zuständigen Schweizer Behörden «aus technischen oder juristischen Gründen» unterblieben ist. Aufgrund dieser Regelung kann eine betroffene Person ihren Kommunikationszugang verlieren, obwohl sie weder eine falsche Identität verwendet noch anderweitig ein Fehlverhalten begangen hat. Dass eine Behörde ein ausländisches Dokument aus rechtlichen oder technischen Gründen nicht erhält, liegt regelmässig ausserhalb des Einflussbereichs der betroffenen Person. Eine so schwere Rechtsfolge darf nicht ausschliesslich an ein administratives oder technisches Problem bei der Datenübermittlung geknüpft werden. Bei den übrigen Sperrgründen muss ausserdem ein rascher und wirksamer Rechtsschutz gewährleistet sein. Betroffene müssen über die Sperrung und deren Begründung informiert werden und eine unkomplizierte Möglichkeit erhalten, ihre Identität nachzuweisen und eine fehlerhafte Sperrung sofort aufheben zu lassen. Absatz 2 entbehrt einer soliden Grundlage: Ob eine ansonsten zwingend vorgesehene Sperre vollzogen wird, soll davon abhängen, ob die betreffende Person beziehungsweise ihr Anschluss gerade geheim überwacht wird. Damit wird nicht die Gefährlichkeit oder Verhältnismässigkeit der Sperre zum entscheidenden Kriterium, sondern das Interesse des Staates an der Fortführung einer Überwachungsmassnahme.
Anhang	

Titel	Art. 6b Sperrung von Telefonnummern und Domain-Namen
Antwortoption	Ablehnung

Anpassungen / Gegenvorschlag	~~1 Die Anbieterinnen von Fernmeldediensten müssen auf Hinweis des Bundesamts für Polizei (fedpol) bei einem begründeten Verdacht auf einen mutmasslichen Betrug nach Artikel 146 des Strafgesetzbuchs (StGB) die betreffende schweizerische Telefonnummer sperren; die Sperrung darf höchstens fünf Tage dauern.~~ ~~2 Absatz 1 gilt auch für die Registerbetreiberinnen einer Domain hinsichtlich der Sperrung eines Domain-Namens zweiter Ebene, der einer Internet-Domain untergeordnet ist, für deren Verwaltung die Schweiz zuständig ist.~~ ~~3 Das Bundesamt für Cybersicherheit (BACS) unterstützt das fedpol bei der Beurteilung d~~Streichung in der vorliegenden Form; eventualiter ~~V~~vor~~aussetzungen nach den Absätzen 1 und 2 und stellt diesem zu diesem Zweck Informationen aus Meldungen nach Artikel 73b des Informationssicherheitsgesetzes vom 18. Dezember 2020 zu.~~ ~~4 Die Staatsanwaltschaft oder das zuständige Gericht kann anordnen, dass die Telefonnummer oder der Domain-Name bis zum Abschluss eines Strafverfahrens gesperrt bleibt.~~ ~~5 Bei der Sperrung von Telefonnummern stellt die zuständige Behörde sicher, dass keine solche erfolgt, sofern ihnen bekannt ist, dass die betroffene Nummer Gegenstand eines Überwachungsauftrags des Dienstes ÜPF ist. In diesen Fällen erfolgt eine Rücksprache mit dem Dienst ÜPF~~gängige richterliche Anordnung vorsehen. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt

Begründung	Artikel 6b erlaubt fedpol, bereits gestützt auf einen «begründeten Verdacht» auf Betrug die Sperrung einer Schweizer Telefonnummer oder eines Domain-Namens für bis zu fünf Tage anzuordnen. Erst für eine länger dauernde Sperrung ist eine Anordnung durch die Staatsanwaltschaft oder ein Gericht vorgesehen. Eine Domain oder Telefonnummer ist jedoch kein blosses technisches Mittel. Sie kann Grundlage geschäftlicher Tätigkeit, journalistischer Arbeit, politischer Kommunikation oder persönlicher Erreichbarkeit bilden. Ihre Sperrung greift unmittelbar in die Kommunikationsmöglichkeiten der Betroffenen ein und kann u.U. Existenzen bedrohen. Grundsätzlich gilt die Unschuldsvermutung bis zu einem Rechtskräfigen Urteil. Der erläuternde Bericht räumt selbst ein, dass Artikel 6b die Kommunikationsfreiheit und bei kommerzieller Nutzung auch die Wirtschaftfreiheit beeinträchtigt und dass die verfassungsrechtliche Grundlage der Regelung noch nicht abschliessend geklärt ist. Anders ausgedrückt: äusserst bedenklich, dass dieser Artikel in der Vernehmlassung steht. Der Rechtsvergleich des Bundes stellt ausserdem selbst fest, dass in den untersuchten Nachbarstaaten keine gleichlautende Regelung existiert, die es Ermittlungsbehörden erlaubt, Nummern bereits bei bloss begründetem Tatverdacht sperren zu lassen. Man möchte ergänzen, dass das nicht wundern sollte, wenn ein Staat die Grundrechte ernst nimmt. Die Piratenpartei betrachtet staatlich angeordnete Sperren von Kommunikationsinfrastruktur grundsätzlich kritisch. Die vorgesehene Sperrung erfolgt hier nicht als klassische DNS-Netzsperre bei den Internetzugangsanbietern, sondern unmittelbar auf Ebene der Registerbetreiberin des Domain-Namens. Dadurch wird ein Domain-Name zentral und grundsätzlich für sämtliche Nutzer ausser Funktion gesetzt. Ein solcher Eingriff kann erhebliche Auswirkungen auf die Kommunikations- und Wirtschaftsfreiheit haben und birgt insbesondere das Risiko von Fehl- und Übersperrungen. Besonders problematisch ist, dass die Sperre den gesamten Domain-Namen trifft. Wird lediglich ein einzelner Dienst, eine Unterseite oder ein Benutzerkonto für betrügerische Zwecke missbraucht, können damit auch sämtliche rechtmässigen Inhalte und Dienste unter derselben Domain unerreichbar werden. Wenn es in der aktuellen Fassung einen grossen Anbieter von beispielsweise Mail-Services treffen sollte, wären u.U. hunderttausende ungerechtfertigt betroffen. Sollte eine kurzfristige Sperrmöglichkeit dennoch eingeführt werden, muss mindestens eine unabhängige richterliche Anordnung gefordert werden; eine Entscheidung der Staatsanwaltschaft darf nicht genügen. Bei akuter Gefahr im Verzug könnte eine eng begrenzte Ausnahme mit sofortiger nachträglicher richterlicher Überprüfung vorgesehen werden. Zusätzlich sind in der Gesetzgebung eine Benachrichtigungspflicht, ein zügiger Beschwerdeweg und eine Haftungsregelung für ungerechtfertigte Sperrungen vorzusehen.
Anhang	

Titel	Art. 13a Abs. 1
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	~~1 Die ComCom, das BAKOM und die Beauftragten nach den Artikeln 12c, 20b, 28a und 58 Absatz 1 können Personendaten, einschliesslich Daten über verwal~~Überarbeitungs~~-~~ und ~~strafrechtliche Verfolgungen oder Sanktionen im Fernmeldebereich, bearbeiten, sofern dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist.~~klare Zweckbindung ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Durch die Revision wird das System der Datenbearbeitung und des behördlichen Informationsaustauschs erheblich ausgeweitet. Der erläuternde Bericht hält ausdrücklich fest, dass künftig auch besonders schützenswerte Daten und Ergebnisse von Profilings im Rahmen der Amtshilfe (Art. 30a und 48d) ausgetauscht werden können. Eine derartige Weitergabe ist grundrechtlich nicht mit dem Austausch gewöhnlicher administrativer Daten vergleichbar. Für besonders schützenswerte Personendaten und Profilingresultate sollten demnach mindestens folgende Voraussetzungen unmittelbar im Gesetz festgehalten werden: strikte Zweckbindung, Erforderlichkeit im Einzelfall, Protokollierung der Übermittlung, angemessene Löschfristen sowie ein Verbot der Weiterverwendung zu sachfremden Zwecken. Eine Auslagerung in eine Verordnung genügt nicht. Besonders problematisch ist zudem, dass der geltende Art. 13b Abs. 2 FMG bei Datenübermittlungen ins Ausland noch ausdrücklich vorsieht, dass die Daten ausschliesslich zur Aufsicht über Fernmeldedienstanbieterinnen und zur Marktbeobachtung verwendet werden dürfen und nicht ohne vorgängige Zustimmung an weitere Behörden oder Stellen weitergegeben werden dürfen. Diese expliziten Zweckbindungs- und Weitergabeschranken werden im Vorentwurf abgeschwächt beziehungsweise nicht in gleicher Klarheit weitergeführt. Gerade bei besonders schützenswerten Personendaten und Profilingresultaten ist eine solche Lockerung nicht vertretbar. Übermittlungen von besonders schützenswerten Personendaten ins Ausland sind zu streichen.
Anhang	

Titel	Art. 13b Sachüberschrift sowie Abs. 1–2bis und 4
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	~~Amts- und Rechtshilfe~~ ~~1 Die ComCom, das BAKOM und die Beauftragten nach den Artikeln 12c, 20b, 28a und 58 Absatz 1 geben Schweizer Behörden diejenigen Personendaten bekannt, die diese zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Sie dürfen Daten über verwal~~Überarbei~~tungs~~- und ~~straf~~rechtliche Verfolgungen oder Sanktionen im Fernmeldebereich bekanntgegeben, wenn die Behörde über eine gesetzliche Grundlage verfügt, die ihnen die Bearbeitung solcher Daten erlaubt.~~ ~~2 Sie können ausländischen Behörden Daten bekanntgeben, die diese zur Ausübung der Aufsicht über Anbieterinnen von Fernmeldediensten benötigen, einschliesslich Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen im Fernmeldebereich. Die Bekanntgabe ist nur zulässig, wenn die ausländische Behörde nach dem Recht ihres Staates an das Amts- oder Berufsgeheimnis gebunden ist.~~ ~~2bis Die Bekanntgabe nach Absatz 2 bedarf der vorgängigen Zustimmung der ComCom, des BAKOM oder eines Beauftragten nach Artikel 12c, 20b, 28a oder 58 Absatz 1 oder muss in einem Staatsvertrag vorgesehen sein.~~ ~~4 Schweizer Behörden geben der ComCom, dem BAKOM und den Beauftragten nach den Artikeln 12c, 20b, 28a und 58 Absatz 1 die für den Vollzug der Fernmeldegesetzgebung erforderlichen Daten, einschliesslich Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen im Fernmeldebereich bekannt~~klare Zweckbindung bzw. Streichung von Abs. 2 in der vorliegenden Form. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Durch die Revision wird das System der Datenbearbeitung und des behördlichen Informationsaustauschs erheblich ausgeweitet. Der erläuternde Bericht hält ausdrücklich fest, dass künftig auch besonders schützenswerte Daten und Ergebnisse von Profilings im Rahmen der Amtshilfe (Art. 30a und 48d) ausgetauscht werden können. Eine derartige Weitergabe ist grundrechtlich nicht mit dem Austausch gewöhnlicher administrativer Daten vergleichbar. Für besonders schützenswerte Personendaten und Profilingresultate sollten demnach mindestens folgende Voraussetzungen unmittelbar im Gesetz festgehalten werden: strikte Zweckbindung, Erforderlichkeit im Einzelfall, Protokollierung der Übermittlung, angemessene Löschfristen sowie ein Verbot der Weiterverwendung zu sachfremden Zwecken. Eine Auslagerung in eine Verordnung genügt nicht. Besonders problematisch ist zudem, dass der geltende Art. 13b Abs. 2 FMG bei Datenübermittlungen ins Ausland noch ausdrücklich vorsieht, dass die Daten ausschliesslich zur Aufsicht über Fernmeldedienstanbieterinnen und zur Marktbeobachtung verwendet werden dürfen und nicht ohne vorgängige Zustimmung an weitere Behörden oder Stellen weitergegeben werden dürfen. Diese expliziten Zweckbindungs- und Weitergabeschranken werden im Vorentwurf abgeschwächt beziehungsweise nicht in gleicher Klarheit weitergeführt. Gerade bei besonders schützenswerten Personendaten und Profilingresultaten ist eine solche Lockerung nicht vertretbar. Übermittlungen von besonders schützenswerten Personendaten ins Ausland sind zu streichen.
Anhang	

Titel	3. Abschnitt: Notkommunikation
Antwortoption	Zustimmung
Anpassungen / Gegenvorschlag	--
Begründung	Eine hochverfügbare Notkommunikation, technische Redundanz und End-to-End-Tests liegen nachdrücklich im öffentlichen Interesse. Gerade ein resilientes Telekommunikationssystem muss auch beim Ausfall einzelner Komponenten oder Anbieter weiter funktionieren. Die vorgeschlagene Rückfallebene und die Systemaufgaben sind deshalb grundsätzlich sinnvoll. Die Vorlage sieht unter anderem ein ausschliesslich der Notkommunikation dienendes Netz, Redundanz, Standortidentifikation, eine Koordinationsstelle sowie eine Test- und Integrationsplattform vor.
Anhang	

Titel	Art. 20 Grundsätze
Antwortoption	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	1 Die Anbieterinnen des öffentlichen Telefondienstes müssen sicherstellen, dass die Kommunikation zwischen den Benutzerinnen und Benutzern und den von den Notdiensten sowie den Hilfs- und Beratungsdiensten betriebenen Zentralen (Notkommunikation) jederzeit möglich ist. 2 Sie müssen dazu insbesondere die Leitweglenkung, die Standortidentifikation und die Redundanz (minimale Rückfallebene) sicherstellen. 3 Der Bundesrat kann nach Abwägung der Interessen der Bevölkerung und der Anbieterinnen sowie unter Berücksichtigung der technischen Entwicklung und der internationalen Harmonisierung: a. die Pflichten nach den Absätzen 1 und 2 auf Anbieterinnen anderer Fernmeldedienste ausdehnen, sofern die Dienste öffentlich zugänglich sind und verbreitet genutzt werden; b. Ausnahmen von den Pflichten nach Absatz 2 vorsehen; c. vorsehen, dass Ortungsfunktionen von Endgeräten ohne ausdrückliche Zustimmung der Benutzerin oder des Benutzers genutzt werden dürfen. -> Bei einer Ortung ohne Einwilligung, werden die betroffenen Personen darüber auf allen bekannten Kommunikationswegen, beispielsweise SMS, E-Mail und Briefpost sofort und automatisiert über die Ortung informiert. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Bei Standortdaten ist weiterhin auf strikte Zweckbindung und Datenminimierung zu achten. Eine Ortung ohne ausdrückliche Einwilligung muss auf tatsächliche Notkommunikation beschränkt bleiben. Um Missbrauch vorzubeugen, sollten bei einer Ortung ohne Einwilligung, die betroffenen Personen darüber auf allen bekannten Kommunikationswegen, beispielsweise SMS, E-Mail und Briefpost sofort und automatisiert darüber informiert werden.
Anhang	

Titel	Art. 20e Schutz der Integrität der Notkommunikation
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	~~1 Die zur Notkommunikation verpflichteten Anbieterinnen von Fernmeldediensten ergreifen Massnahmen zum Schutz der Integrität der Notkommunikation.~~ ~~2 Sie stützen sich dabei insbesondere auf die Hinweise der Koordinationsstelle nach Artikel 20a Buchstabe d. Die Anbieterinnen ergreifen die Massnahmen umgehend und so lange wie nötig.~~ ~~3 Sie dürfen Benutzerinnen und Benutzer zum Zweck nach Absatz 1 vom Netz trennen.~~ ~~4 Der Bundesrat legt die technischen und organisatorischen Massnahmen fest, welche die Anbieterinnen nach Absatz 1 treffen müssen~~Änderung von Absatz 3: Netztrennung nur bei unmittelbarer erheblicher Gefährdung und als ultima ratio. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Dass Fernmeldedienstanbieterinnen auf technische Angriffe oder massenhaft fehlerhaft ausgelöste Notrufe reagieren können müssen, ist unbestritten. Der erläuternde Bericht nennt beispielsweise Geräte, die wegen fehlerhafter Sensoren wiederholt falsche Notrufe auslösen. Absatz 3 erlaubt den Anbieterinnen jedoch sehr pauschal, Nutzerinnen und Nutzer vom Netz zu trennen. Eine vollständige Netztrennung ist ein gravierender Eingriff und kann gerade die Möglichkeit nehmen, selbst einen echten Notruf abzusenden. Das Gesetz sollte daher festhalten, dass eine Netztrennung nur zulässig ist, wenn eine unmittelbare und erhebliche Gefährdung der Notkommunikation vorliegt, mildere technische Massnahmen nicht ausreichen und die Trennung auf die kürzest mögliche Dauer beschränkt bleibt. Soweit technisch machbar, sollte lediglich die störende Funktion oder Kommunikation blockiert werden und nicht der gesamte Fernmeldezugang. Der Massnahmenkatalog sollte Kategorisiert werden, unter anderem auch nach Sensorik und Anwendungsbereiche: - Brandmeldeanlagen / Rauchmelder - Einbruchs-Alarmsysteme - Wasserbruchmelder - etc.
Anhang	

Titel	Art. 29
Antwortoption	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	~~1 Die Inhaberinnen und Inhaber von Adressierungselementen und die Beauftragten nach Artikel 28a sind verpflichtet, der zuständigen Behörde die zur Verwaltung der zugeteilten Adressierungselemente notwendigen Auskünfte zu erteilen.~~ ~~2 Für Cybersicherheit zuständige anerkannte private und öffentliche Stellen können untereinander und mit den Beauftragten nach Artikel 28a zusammenarbeiten, um Gefährdungen durch Cyberbedrohungen festzustellen und zu beurteilen.~~ ~~3 Der Bundesrat legt die Kriterien für die Anerkennung der privaten und öffentlich~~Sicherstellen, dass es nicht zu einem allgemeinen Austausch personenbezogener Daten zwischen staatlichen und privaten Stellen f~~es~~führt. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Die Zusammenarbeit zwischen Cybersicherheitsstellen sowie der Austausch technischer Indikatoren wie Malware-Signaturen, Angriffsmustern oder Informationen über Sicherheitslücken sind sinnvoll und ausdrücklich zu begrüssen. Dabei muss jedoch sichergestellt werden, dass die Zusammenarbeit tatsächlich auf die Bekämpfung konkreter Cyberbedrohungen beschränkt bleibt und nicht zu einem allgemeinen Austausch personenbezogener Daten zwischen staatlichen und privaten Stellen führt.
Anhang	

Titel	Art. 30a Datenbearbeitung sowie Amts- und Rechtshilfe
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	Abs. 1 und 2: Streichung bzw. Beschränkung auf rein technische Daten. 1 Das BAKOM und die Beauftragten nach Artikel 28a sind befugt, für die Erfüllung der Aufgaben nach Artikel 28d Buchstabe a und die Umsetzung von Artikel 28e Buchstabe c Profilings durchzuführen, nötigenfalls auch ohne Wissen der betroffenen Personen, und dabei die folgenden besonders schützenswerten Personendaten zu bearbeiten: a. biometrische Daten, die eine natürliche Person eindeutig identifizieren; b. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen. 2 Sie können diese Daten und Resultate von Profilings den für den Schutz vor Cyberbedrohungen zuständigen Schweizer Behörden und anderen für Cybersicherheit anerkannten privaten und öffentlichen Stellen bekanntgeben, sofern diese Behörden im Rahmen der Erfüllung von Aufgaben im Bereich des Schutzes vor Cyberbedrohungen über eine entsprechende gesetzliche Grundlage verfügen. Abs. 3: Streichung der Delegation; die wesentlichen Schranken direkt ins Gesetz. 3 Der Bundesrat regelt die Einzelheiten der Bearbeitung besonders schützenswerter Personendaten und der Durchführung von Profilings. 4 Die Artikel 13a und 13b sind auf die Bearbeitung dieser Daten und auf ihre Bekanntgabe an schweizerische oder ausländische Behörden anwendbar. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt

Begründung	Abs. 1 und 2 Es ist gänzlich unverständlich, weshalb für die Bekämpfung von Cyberbedrohungen eine allgemeine gesetzliche Grundlage geschaffen werden soll, welche die Bearbeitung biometrischer Daten und die Durchführung von Profilings ermöglicht – nötigenfalls sogar ohne Wissen der betroffenen Personen. Artikel 30a nennt ausdrücklich biometrische Daten zur eindeutigen Identifikation natürlicher Personen sowie Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen. Der Bericht (S. 44) räumt gleichzeitig selbst ein, dass der überwiegende Teil der für die Cybersicherheit erforderlichen Analysen gerade keine Personendaten benötigt, sondern auf technischen Daten, Malware-Merkmalen und Angriffsmustern beruht. Damit fehlt eine überzeugende Begründung für eine derart weitreichende Vorratskompetenz. Staatliches Profiling natürlicher Personen und insbesondere die Verarbeitung biometrischer Daten dürfen nicht vorsorglich ermöglicht werden, nur weil eine mögliche zukünftige Verwendung solcher Instrumente nicht ausgeschlossen werden kann. Der eigentliche Zweck scheint einmal mehr zu sein, die Bevölkerung präventiv stärker zu überwachen. Dies gilt umso mehr, als der Bericht ausdrücklich auch den Einsatz von Scoring-Verfahren und künstlicher Intelligenz zur Vorhersage einer möglichen missbräuchlichen Nutzung von Domain-Namen vorsieht. Eine solche automatisierte Bewertung von Personen und deren digitalem Verhalten steht in einem fundamentalen Spannungsverhältnis zum Recht auf Digitale Integrität und insbesondere zum Recht, nicht von einer Maschine beurteilt sowie nicht unverhältnismässig überwacht, vermessen oder analysiert zu werden. Abs. 3 Besonders problematisch ist, dass die konkrete Ausgestaltung der Bearbeitung besonders schützenswerter Personendaten und der Durchführung von Profilings gemäss Absatz 3 weitgehend dem Bundesrat überlassen werden soll. Bei Eingriffen dieser Tragweite dürfen zentrale Fragen wie die zulässigen Datenkategorien, der Umfang des Profilings, die Verknüpfung verschiedener Datenquellen, Aufbewahrungsfristen, Transparenzpflichten und die Rechte betroffener Personen nicht erst auf Verordnungsstufe festgelegt werden. Angesichts der Schwere dieser Grundrechtseingriffe müssen die wesentlichen Voraussetzungen und Grenzen mindestens auf Gesetzesstufe geregelt sein. Der aus Sicht der Piratenpartei konsequentere Weg wäre jedoch, die Bearbeitung biometrischer Daten und das Profiling natürlicher Personen aus Artikel 30a vollständig zu streichen und die Bestimmung auf jene technischen Daten zu beschränken, die für die Abwehr konkreter Cyberbedrohungen tatsächlich erforderlich und nützlich sind.
Anhang	

Titel	Art. 34a Lokalisierung von Störungen
Antwortoption	Ablehnung

Anpassungen / Gegenvorschlag	~~1 Um den Ursprung von Störungen des Fernmeldeverkehrs oder des Rundfunks oder einer Stark- oder Schwachstromanlage zu bestimmen, ist dem BAKOM Zugang zu allen Fernmeldeanlagen sowie Stark- und Schwachstromanlagen zu gewähren. Auf Verlangen müssen die Anbieterinnen, Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten dem BAKOM die Gesamtheit der relevanten technischen Informationen betreffend den massgeblichen Zeitraum, insbesondere zu den Abstrahlungseigenschaften und den Abstrahlungs-einstellungen der betroffenen Funkanlage, zur Verfügung stellen.~~ ~~2 Das BAKOM kann Fahrzeuge, bei denen ein Störsignal festgestellt wird, zur Identifikation automatisiert optisch erfassen, gegebenenfalls anhalten lassen und kontrollieren. Die dabei erfassten Daten werden unverzüglich gelöscht, sofern sie nicht als Beweismittel benötigt werden.~~ ~~3 Der Bundesrat regelt die Einzelheiten betreffend das zu beschaffende System für die automatisierte optische Erfassung sowie die Anonymisierungsvoraussetzungen und legt die Aufbewahrungsdauer für Daten fest, die als Beweismittel benötigt werden.~~ ~~4 Das BAKOM regelt die Einzelheiten betreffend die Pflicht, Informationen auf Verlangen zur Verfügung zu stelle~~Automatisierte optische Fahrzeugerfassung streichen oder die Voraussetzungen, den Umfang der Datenerhebung und die Aufbewahrung unmittelbar und abschliessend im Gesetz regeln. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt

Begründung	Die technische Lokalisierung von Funkstörungen wie es Art. 34a vorsieht, ist eine berechtigte Aufgabe des BAKOM. Problematisch ist jedoch die neu vorgesehene Möglichkeit, Fahrzeuge automatisiert optisch zu erfassen, gegebenenfalls anhalten zu lassen und zu kontrollieren. Artikel 34a Absatz 2 beschränkt die Erfassung zwar auf Fahrzeuge, bei denen ein Störsignal festgestellt wurde. Der Bericht zeigt jedoch, dass damit eine Fülle personenbezogener Fahrzeugdaten verbunden ist: Neben Datum, Zeit und Ort sollen Fahrzeugtyp, Fahrzeugmarke, Kontrollschild und gegebenenfalls die Fahrzeugfarbe automatisiert erfasst werden (S. 52). Damit geht es nicht bloss um eine technische Frequenzmessung, sondern um ein System, das ein konkretes Fahrzeug identifizierbar macht und dessen Anwesenheit zu einem bestimmten Zeitpunkt an einem bestimmten Ort dokumentiert. Die Vorlage sieht zwar vor, die erfassten Daten unverzüglich zu löschen, sofern sie nicht als Beweismittel benötigt werden. Wesentliche Schutzvorkehrungen, insbesondere die konkrete Ausgestaltung des Erfassungssystems, die Anonymisierung und die Aufbewahrungsdauer, sollen jedoch erst durch den Bundesrat auf Verordnungsstufe geregelt werden. Der erläuternde Bericht geht zudem ausdrücklich davon aus, dass falsch positive Ergebnisse auftreten können (S. 54). Nicht verwertbare Aufnahmen sowie Aufnahmen unbeteiligter Fahrzeuge sollen deshalb erst nach einer nachgelagerten Prüfung ausgesondert und gelöscht werden. Bei einer vermuteten absichtlichen Störung können die Daten dagegen bis zum Abschluss des Verwaltungsstrafverfahrens gespeichert werden. Grundsätzlich möchten wir festhalten, dass mit dieser Massnahme erstmal alle Fahrzeuge automatisiert erfasst werden und dann erst entschieden wird, ob das Fahrzeug vom Zweck dieses Artikels betroffen ist. Dann wird aussortiert. Dies bedeutet jedoch auch, dass die entsprechende Infrastruktur vorhanden ist und auch definitiv unschuldige, wenn auch nur kurzfristig, erfasst werden. Auch wenn die Daten sofort wieder gelöscht werden ist zu erwarten, dass beispielsweise Logging-Daten bei der Abfrage entstehen usw.. Es stellt sich die Frage, inwiefern die Verhältnismässigkeit dieses Grundrechtseingriffs überhaupt gegeben ist. Nichtsdestotrotz gehören die wesentlichen Grenzen dieser Datenerhebung auf Gesetzesstufe. Insbesondere sollte ausdrücklich festgehalten werden, dass: - die Erfassung ausschliesslich aufgrund eines zuvor technisch festgestellten konkreten Störsignals ausgelöst werden darf; - nur die für die Identifikation des störungsverursachenden Fahrzeugs zwingend erforderlichen Daten erhoben werden dürfen; - keine permanente, flächendeckende oder anlasslose Fahrzeugerfassung zulässig ist; - Daten unbeteiligter Fahrzeuge und falsch positive Erfassungen unverzüglich nach ihrer Erkennung gelöscht werden; - keine allgemeine Fahrzeug- oder Bewegungsdatenbank aufgebaut werden darf; - keine Verknüpfung mit anderen Datenbeständen zu sachfremden Zwecken erfolgen darf; - für als Beweismittel gespeicherte Daten eine gesetzliche maximale Aufbewahrungsdauer vorgesehen wird. Der Bericht begründet die Verhältnismässigkeit der Massnahme ausdrücklich auch damit, dass die Überwachung nicht permanent, sondern lediglich stichprobenartig erfolgen soll und die vorgesehenen Messstellen nicht fest installiert seien. Wenn diese Beschränkungen Voraussetzung für die behauptete Verhältnismässigkeit sind, müssen sie auch im Gesetz verbindlich festgeschrieben werden und dürfen nicht bloss im Bericht stehen.
Anhang	

Titel	Art. 46 Abs. 2
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	~~2 Er kann nach Abwägung der Interessen der Bevölkerung, der angerufenen und anrufenden Personen sowie der Anbieterinnen u~~Anwe~~nd~~ ~~un~~ter Berücksichtigung der technischen Entwicklung und der internationalen Harmonisierung Ausnahmen festlegen und für Festnetzanschlüsse der Polizei, der Feuerwehr, der Sanitäts- und Rettungsdienste sowie der Hilfs- und Beratungsdienste die Aufhebung der Rufnummernunterdrückung auch ohne ausdrückliche Zustimmung der anrufenden Teilnehmerinnen und Teilnehmer vorseh~~~~gsfälle abschliessend im Gesetz festlege~~n. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Die Möglichkeit, die Unterdrückung einer Telefonnummer aufzuheben, tangiert die Privatsphäre der anrufenden Person. Bei eigentlichen Notrufen ist die Übermittlung der Rufnummer nachvollziehbar. Der neue Artikel dehnt diese Ausnahme jedoch auf reguläre Festnetzanschlüsse von Polizei, Feuerwehr, Sanitäts- und Rettungsdiensten sowie Hilfs- und Beratungsdiensten aus. Damit wird eine heute bewusst bestehende Schutzfunktion für eine nach oben offene Menge von Anschlüssen beseitigt. Solche Ausnahmen sollten abschliessend auf Gesetzesstufe benannt und auf Situationen beschränkt werden, in denen ein überwiegendes Sicherheitsinteresse besteht. Gerade bei Hilfs- und Beratungsdiensten kann die Anonymität für Betroffene selbst Teil der Schutzfunktion des Angebots sein.
Anhang	

Titel	Art. 46a Kinder- und Jugendschutz
Antwortoption	Ablehnung
Anpassungen / Gegenvorschlag	~~1 Die Anbieterinnen von Internetzugängen müssen ihre Kundinnen und Kunden über die Möglichkeiten im Bereich des Kinder- und Jugendschutzes beraten und ihnen Mittel bieten, mit denen Kinder und Jugendliche wirksam vor pornografischen Inhalten geschützt werden können.~~ ~~2 Der Bundesrat kann weitere Vorschriften zum Schutz von~~Zustimmung zu Absatz 1; Streichung von Absatz 2 oder mindestens enger fassen. K~~ind~~e~~ern und Jugendlichen vor den Gefahren, die sich aus de~~e Grundlage für N~~ue~~tz~~u~~ng der Fernmeldedienste ergeben, erlassen.~~ ~~3 Damit Informationen mit pornograf~~sperren, systematischem~~ Inhalt ~~nach Artikel 197 Absätze 4 und 5 des Strafgesetzbuchs rasch und weltweit gelöscht werden, koordinieren das BAKOM, fedpol und die zuständigen Stellen in den Kantonen geeignete Massnahmen. Dazu können von Dritten betriebene Meldestellen sowie Behörden im Ausland beigezogen und unterstützt werden. Der Bundesrat regelt die Einzelheiten.~~ ~~4 Die Anbieterinnen von Fernmeldediensten unterdrücken die Informationen mit pornografischem Inhalt nach Artikel 197 Absätze 4 und 5 StGB, auf die fedpol sie hinweist. Die Anbieterinnen von Fernmeldediensten melden fedpol Verdachtsfälle über Informationen mit pornografischem Inhalt nach Artikel 197 Absätze 4 und 5 des Strafgesetzbuchs, auf die sie im Rahmen ihrer Tätigkeit zufällig gestossen sind oder auf die sie von Dritten schriftlich hingewiesen wurd~~überwachung oder allgemeine Identifikations- und Altersverifikationspflichten schaffen. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Absatz 1 verpflichtet Anbieterinnen von Internetzugängen, ihre Kundinnen und Kunden über Möglichkeiten des Kinder- und Jugendschutzes zu beraten und entsprechende Schutzmittel anzubieten. Der erläuternde Bericht nennt dabei insbesondere technische Möglichkeiten auf Endgeräten sowie Tools und Apps. Dieser Ansatz ist grundsätzlich zu begrüssen. Absatz 2 ermächtigt den Bundesrat jedoch sehr allgemein, weitere Vorschriften zum Schutz von Kindern und Jugendlichen zu erlassen, ohne deren mögliche Eingriffsintensität näher zu begrenzen. Daraus darf keine Verpflichtung entstehen, den Internetverkehr systematisch zu analysieren, Verschlüsselung aufzubrechen, zentrale Filter- oder Sperrinfrastrukturen aufzubauen oder sämtliche Nutzerinnen und Nutzer zu identifizieren beziehungsweise ihr Alter zu verifizieren. Jugendschutz sollte soweit möglich auf Ebene der Endgeräte und unter Kontrolle der Nutzerinnen, Nutzer und Erziehungsberechtigten umgesetzt werden. Dabei dürfen Endgeräte jedoch nicht zu Kontrollpunkten für eine verpflichtende Inhaltsanalyse werden. Insbesondere darf keine Grundlage für ein anlassloses automatisiertes Durchsuchen privater Kommunikation geschaffen werden – auch nicht durch sogenanntes Client-Side-Scanning, bei dem Inhalte direkt auf dem Endgerät vor oder nach der Verschlüsselung analysiert werden (vgl. Chatkontrolle).
Anhang	

Titel	Art. 48a Resilienz der Fernmeldeinfrastrukturen und Schutz vor Cyberbedrohungen
Antwortoption	Ablehnung

Anpassungen / Gegenvorschlag	~~1 Die Anbieterinnen von Fernmeldediensten müssen technische, operative und administrative Massnahmen ergreifen, um die unbefugte Manipulation von Fernmeldeinfrastrukturen dur~~Absatz 3 bezügli~~ch f~~V~~er~~~~nmeldetechnische Übertragungen zu bekämpfen, um die Resilienz der Fernmeldeinfrastrukturen zu verbessern und um vor Cyberbedrohungen zu schützen. Sie sind zu diesem Zweck be~~kehrsdaten stre~~ch~~tigt, Verbindungen umzuleiten oder zu verhindern und Informationen zu unterdrücken.~~ ~~2 Das BAKOM überwacht, ermittelt und bewertet Risikofaktoren, welche die Resilienz der Fernmeldeinfrastrukturen gefährden oder den Schutz vor Cyberbedrohungen beinträchtigen können. Es evaluiert dabei insbesondere das Vorliegen eines Sicherheitsrisikos für die Fernmeldeinfrastrukturen nach Artikel 48b.~~ ~~3 Die Anbieterinnen von Fernmeldediensten haben dem BAKOM die zur Erfüllung seiner Aufgaben nach Absatz 2 notwendigen Auskünfte, einschliesslich der Verkehrsdaten, bekannt zu geben, sofern sie darüber verfügen. Sie können untereinander und mit für Cybersicherheit zuständigen anerkannten privaten und öffentlichen Stellen zusammenarbeiten, um Gefährdungen durch Cyberbedrohungen festzustellen und zu beurteilen.~~ ~~4 Der Bundesrat präzisiert die Massnahmen nach Absatz 1. Er kann zum Schutz vor Gefahren, zur Vermeidung von Schäden und zur Minimierung von Risiken Bestimmungen über die Sicherheit von Informationen sowie von Fernmeldeinfrastrukturen und -diensten erlassen, insbesondere bezüglich:~~ ~~a. Verfügbarkeit;~~ ~~b. Betrieb;~~ ~~c. Sicherstellung von redundanten Infrastrukturen;~~ ~~d. Meldung von Störungen;~~ ~~e. Nachvollziehbarkeit von Vorgängen;~~ ~~f. Umleitung oder Verhinderung von Verbindungen sowie Unterdrückung von Informationen nach Absatz 1~~ en oder deutlich einschränken; die Kompetenzen nach Absätzen 2 und 4 eng auf technische Sicherheitszwecke begrenzen; die Befugnis zur «Unterdrückung von Informationen» in Absatz 1 und 4 klar eingrenzen. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt

Begründung	Absatz 1 verpflichtet die Anbieterinnen zu technischen, operativen und administrativen Massnahmen gegen Cyberbedrohungen und zur Verbesserung der Resilienz. Dies ist grundsätzlich zu begrüssen. Im Rahmen der vorliegenden Revision ist aber kritisch zu hinterfragen, dass Art. 48a die bereits bestehende, sehr weit gefasste Befugnis zur «Unterdrückung von Informationen» unverändert in den erheblich ausgebauten Regelungsbereich zu Resilienz und Cyberbedrohungen übernimmt. Der Begriff bleibt technisch und materiell weitgehend unbestimmt und kann je nach Umsetzung faktisch eine Sperrung von Inhalten bedeuten. Damit geht es nicht bloss um den Schutz technischer Infrastruktur oder die Unterbrechung schädlicher Verbindungen, sondern potenziell unmittelbar um die Zugänglichkeit von Informationen. Gerade im Zuge einer Revision, welche die Kompetenzen im Bereich der Cybersicherheit erheblich erweitert, sollte deshalb gesetzlich präzisiert werden, was unter «Unterdrückung» zu verstehen ist, unter welchen Voraussetzungen sie zulässig ist und welche technischen Verfahren eingesetzt werden dürfen. Bei behördlich veranlassten Eingriffen in die Zugänglichkeit von Inhalten sind zudem wirksamer Rechtsschutz und unabhängige richterliche Kontrolle vorzusehen. Absatz 2 überträgt dem BAKOM neu die Aufgabe, Risikofaktoren für Fernmeldeinfrastrukturen zu überwachen, zu ermitteln und zu bewerten. Diese Aufgabe sollte auf sicherheitsrelevante technische, organisatorische und infrastrukturelle Risiken, einschliesslich Lieferketten, Abhängigkeiten und Kontrollverhältnissen beschränkt bleiben und nicht zu einer allgemeinen Überwachung von Kommunikationsverhalten führen. Besonders kritisch ist Absatz 3: Anbieterinnen müssen dem BAKOM die zur Erfüllung dieser Aufgaben erforderlichen Auskünfte «einschliesslich der Verkehrsdaten» bekanntgeben. Gleichzeitig erlaubt die Bestimmung den Informationsaustausch mit anerkannten privaten und öffentlichen Cybersicherheitsstellen. Verkehrsdaten erlauben weitreichende Rückschlüsse auf Kommunikationsbeziehungen und Verhalten. Der Hinweis des Berichts, Kommunikationsinhalte blieben weiterhin geschützt, beseitigt die Grundrechtsrelevanz dieser Metadaten nicht. Die Herausgabe von Verkehrsdaten darf deshalb höchstens bei einem konkreten Sicherheitsereignis und soweit unbedingt erforderlich zulässig sein. Eine pauschale oder präventive Übermittlung zur abstrakten Risikobeobachtung lehnen wir ab. Wo möglich, sind aggregierte oder anonymisierte technische Daten zu verwenden. Absatz 4 ermächtigt den Bundesrat zudem, die Sicherheitsmassnahmen weiter zu konkretisieren, unter anderem bezüglich Nachvollziehbarkeit von Vorgängen sowie Umleitung oder Verhinderung von Verbindungen. Auch diese Delegation darf nicht dazu führen, dass grundrechtsrelevante Überwachungs- oder Datenbearbeitungsbefugnisse erst auf Verordnungsstufe geschaffen werden.
Anhang	

Titel	Art. 48b Sicherheit von Fernmeldeinfrastrukturen
Antwortoption	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	~~Einfügen vor dem Gliederungstitel des 9. Kapitels~~ ~~1 Die Anbieterinnen von Fernmeldediensten müssen Fernmeldeinfrastrukturen nutzen, welche die Vertraulichkeit, die Integrität und die Verfügbarkeit von Fernmeldediensten gewährleisten. Die Sicherheitseinstellungen müssen standardmässig konfiguriert und aktiviert sein und auf dem neusten Stand gehalten w~~Kriterien für Verbote präzisieren~~.~~ ~~2 Die kritischen Bestandteile der Fernmeldeinfrastruktur einer Anbieterin von Fernmeldediensten müssen von verschiedenen Herstellerinnen stammen, wobei mindestens eine Herstellerin in einem Staat einen Sitz haben muss, dessen Gesetzgebung einen angemessenen Datenschutz gewährleistet. Der Bundesrat regelt die Einzelheiten; er kann Kategorien, Anteile und Mindestprozentsätze festlegen.~~ ~~3 Stellt das BAKOM ein begründetes Sicherheitsrisiko fest, so verbietet es den Anbieterinnen von Fernmeldediensten, betroffene Bestandteile in Betrieb zu nehmen. Es veröffentlicht eine Liste der verbotenen Bestandteile. Es kann die Ausserbetriebnahme oder Entfernung verbotener Bestandteile verfügen. Bei Bestandteilen, die für die Fernmeldeüberwachung nach dem BÜPF von Belang sind, nimmt das BAKOM vorgängig Rücksprache mit dem Dienst ÜPF~~ und Rechtsschutz gewährleisten. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt
Begründung	Die Grundidee des Artikels von «Security by Design and by Default», laufenden Sicherheitsupdates und der Verminderung einseitiger technologischer Abhängigkeiten ist ausdrücklich zu begrüssen. Auch eine Diversifizierung kritischer Komponenten kann die Resilienz erhöhen. Der Entwurf sieht für kritische Bestandteile eine Mehrlieferantenstrategie vor und verlangt, dass mindestens eine Herstellerin ihren Sitz in einem Staat mit angemessenem Datenschutz hat. Die Sicherheit darf jedoch nicht ausschliesslich nach Herkunft oder Unternehmenssitz beurteilt werden. Massgeblich sein müssen überprüfbare technische Eigenschaften, Sicherheitspraktiken, Lieferketten, Kontrollverhältnisse und konkrete Risiken. Wo möglich, sind transparente und unabhängig auditierbare Lösungen zu bevorzugen; offen einsehbarer Quellcode und FOSS können hierzu einen wesentlichen Beitrag leisten. Absatz 3 sehen wir allerdings kritisch. Nach diesem kann das BAKOM bei einem von ihm festgestellten «begründeten Sicherheitsrisiko» Bestandteile verbieten beziehungsweise deren Entfernung anordnen kann. Hersteller und Betreiber müssen vor einem solchen Entscheid angehört werden und der Entscheid muss anfechtbar sein.
Anhang	

Titel	Art. 48c Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken
Antwortoption	Ablehnung

Anpassungen / Gegenvorschlag	~~1 Der Bundesrat kann den Anbieterinnen von Fernmeldediensten den Erwerb, die Inbetriebnahme und den Betrieb von Bestandteilen von Fernmeldeinfrastruktur verbieten, die von Herstellerinnen stammen, die für die Schweiz ein geopolitisches Risiko darstellen oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der für die Schweiz ein geopolitisches Risiko darstellt.~~ ~~2 Er berücksichtigt bei der Beurteilung des geopolitischen Risikos die innere und äussere Sicherheit sowie den Schutz des Werk-, Wirtschafts- und Finanzplatzes der Schweiz unter Einbezug:~~ ~~a. der direkt oder indirekt verhängten Sanktionen gegen die Herstellerinnen nach dem Embargogesetz vom 22. März 2002;~~ ~~b. der wirtschaftlichen, technologischen und sicherheitsbezogenen Abhängigkeiten in Bezug auf die Herstellerinnen oder die Lieferkette;~~ ~~c. der sicherheitsrelevanten Gefährdungslage durch Cyberangriffe, Sabotage und nachrichtendienstliche Aktivitäten;~~ ~~d. der Androhung von Sanktionen oder Embargos, die die Sicherheit oder die Wirtschaft der Schweiz beeinträchtigen würden.~~ ~~3 Der Bundesrat kann die Anbieterinnen von Fernmeldediensten verpflichten, Bestandteile, die von Herstellerinnen nach Absatz 1 stammen, aus ihrer Fernmeldeinfrastruktur zu entfernen. Er trägt dabei den wirtschaftlichen Auswirkungen Rechn~~Allgemein: Änderung: Kompetenz des Bundesrats deutlich enger fassen und parlamentarische Kontrolle vorsehen. Art. 48c Abs. 2 Bst. d: Streichung. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt

Begründung	Allgemein Art. 48c will die Infrastruktur vor geopolitischen Risiken schützen: Die Schweiz darf bei kritischer Infrastruktur nicht von einzelnen Staaten oder Herstellern in einer Weise abhängig werden, die Erpressung, Sabotage oder die Unterbrechung zentraler Dienste ermöglicht. Artikel 48c räumt dem Bundesrat allerdings eine sehr weitreichende Kompetenz ein, gestützt auf eine eigene geopolitische Risikobeurteilung den Erwerb, die Inbetriebnahme oder den Betrieb von Komponenten bestimmter Hersteller zu verbieten und sogar die Entfernung bereits installierter Komponenten anzuordnen. Solche Entscheide können erhebliche wirtschaftliche und aussenpolitische Auswirkungen haben und dürfen nicht zu einem politisch motivierten Instrument gegen Hersteller aus missliebigen Staaten degenerieren. Positiv ist, dass mehrere neutral-begründbare Kriterien – Abhängigkeiten, Cyberangriffe, Sabotage und nachrichtendienstliche Aktivitäten – im Gesetz genannt sind. Die Anwendung sollte ausserdem an eine konkret festgestellte erhebliche Gefährdung geknüpft werden. Anbieter und Hersteller müssen angehört werden und Zugang zu einem gerichtlichen Rechtsmittel erhalten. Bei weitreichenden Massnahmen sollte zudem eine parlamentarische Kontrolle vorgesehen werden. Der erläuternde Bericht weist selbst darauf hin, dass zu prüfen sein wird, ob Artikel 48c in den Anhang des Parlamentsgesetzes über bundesrätliche Krisenverordnungen aufgenommen werden soll (S. 65). Das sollte unbedingt geschehen. Art. 48c Abs. 2 Bst. d Die «Androhung von Sanktionen oder Embargos» ist als Kriterium für die Beurteilung eines geopolitischen Risikos zwar verständlich, dennoch aber fragwürdig. Der Wortlaut unterscheidet weder danach, von welchem Staat die Drohung ausgeht, noch aus welchem Anlass sie ausgesprochen wird. Damit könnte grundsätzlich auch die Drohung eines mächtigen Drittstaates wie der USA oder China mit wirtschaftlichen Sanktionen berücksichtigt werden, wenn die Schweiz Produkte eines Herstellers dieses Staates verbieten möchte. Damit besteht die Gefahr eines problematischen Zirkelschlusses: Je glaubwürdiger ein ausländischer Staat wirtschaftlichen oder politischen Druck auf die Schweiz ausüben kann, desto stärker könnte dieser Druck selbst die Entscheidung über die Zulässigkeit seiner Technologien beeinflussen. Gerade eine Regelung, welche die technologische und geopolitische Unabhängigkeit der Schweiz stärken soll, sollte ausländische Erpressungsversuche nicht einfach als gewöhnliches Kriterium in eine Interessenabwägung einbeziehen. Soll die Androhung von Sanktionen oder Embargos überhaupt berücksichtigt werden, dann müsste sie vielmehr gegen diejenige technologische Abhängigkeit sprechen, über welche ein ausländischer Staat solchen Druck auf die Schweiz ausüben kann. Wer versucht, die Schweiz durch die Androhung von Sanktionen oder Embargos zur Nutzung bestimmter Technologien zu zwingen, liefert damit selbst den stärksten Grund dafür, diese Abhängigkeit zu beenden und die betreffenden Komponenten auszuschliessen. Falls Buchstabe d beibehalten wird, ist deshalb unbedingt gesetzlich klarzustellen, dass damit nur Risiken gemeint sind, die aus der Nutzung bzw. Abhängigkeit von einer bestimmten Infrastruktur entstehen, nicht Sanktionen oder Embargos, die als Reaktion auf einen souveränen Regulierungsentscheid der Schweiz angedroht werden.
Anhang	

Titel	Art. 48d Bearbeitung von Daten und Zusammenarbeit
Antwortoption	Ablehnung

Anpassungen / Gegenvorschlag	~~1 Das BAKOM ist befugt, für die Erfüllung der Aufgaben nach den Artikeln 48a und 48b Profilings durchzuführen, nötigenfalls auch ohne Wissen der betroffenen Personen, und dabei die folgenden besonders schützenswerten Personendaten zu bearbeiten:~~ ~~a. biometrische Daten, die eine natürliche Person eindeutig identifizieren;~~ ~~b. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen.~~ ~~2 Das BAKOM kann diese Daten und Resultate von Profilings den für den Schutz vor Cyberbedrohungen zuständigen Schweizer Behörden und anderen für Cybersicherheit anerkannten privaten und öffentlichen Stellen nach Artikel 29 bekanntgeben, sofern diese Behörden im Rahmen der Erfüllung von Aufgaben im Bereich des Schutzes vor Cyberbedrohungen über eine entsprechende gesetzliche Grundlage verfügen.~~ ~~3 Die Anbieterinnen von Fernmeldediensten können untereinander und mit für Cybersicherheit anerkannten privaten und öffentlichen Stellen nach Artikel 29 zusammenarbeiten, um Gefährdungen durch Cyberbedrohungen festzustellen und zu beurteilen.~~ ~~4 Der Bundesrat regelt die Einzelheiten der Bearbeitung besonders schützenswerter Personendaten sowie der Durchführung von Profilings.~~ ~~5 Die Artikel 13a und 13b sind auf die Bearbeitung dieser Daten durch das BAKOM und auf ihre Bekanntgabe an schweizerische oder ausländische Behörden anwendbar~~Streichung. ~~Gelöschter Inhalt~~ Geänderter oder ergänzter Inhalt

Begründung	Artikel 48d zählt aus grundrechtlicher Sicht zu den problematischsten Bestimmungen der Vorlage. Das BAKOM soll Profilings durchführen dürfen, nötigenfalls ohne Kenntnis der betroffenen Personen, und dabei biometrische Daten zur eindeutigen Identifizierung sowie Daten über verwaltungs- und strafrechtliche Verfolgungen und Sanktionen bearbeiten können. Diese Daten und die Resultate der Profilings können anschliessend weiteren Behörden sowie anerkannten privaten oder öffentlichen Cybersicherheitsstellen mitgeteilt werden. Der Bericht rechtfertigt die Regelung damit, dass solche Daten beispielsweise notwendig sein könnten, um Cyberangreifer zu identifizieren oder Risikoprofile zu erstellen. Gleichzeitig wird ausdrücklich festgehalten, dass sich der überwiegende Teil von Cyberbedrohungsanalysen "nicht auf Personendaten [stützt]" (S. 65). Aus einzelnen denkbaren Anwendungsfällen lässt sich jedoch keine weitreichende gesetzliche Ermächtigung zu staatlichem Profiling ohne Wissen der betroffenen Personen und zur Bearbeitung biometrischer Daten ableiten. Besonders problematisch ist entsprechend auch die Argumentation auf Seite 66, wonach heute noch nicht bestimmt werden könne, welche Daten für ein Profiling erforderlich und welche Formen des Profilings künftig nützlich sein würden, und deshalb der Bundesrat die Einzelheiten regeln solle. Diese Argumentation ist rechtsstaatlich geradezu widersinnig: Je weniger heute über Art und Umfang eines künftigen Grundrechtseingriffs bekannt ist, desto weniger eignet sich diese Unbestimmtheit als Rechtfertigung für eine weit gefasste gesetzliche Ermächtigung. Aus grundrechtlicher Sicht müsste genau die entgegengesetzte Schlussfolgerung gezogen werden: Solange Art und Umfang eines Eingriffs nicht hinreichend bestimmt werden können, darf keine weit gefasste Ermächtigung geschaffen werden. Soweit die Bearbeitung besonders schützenswerter Personendaten und das Profiling im konkreten Fall nicht nachweislich erforderlich sind, können die Eingriffe bereits die Voraussetzung der Verhältnismässigkeit nach Art. 36 Abs. 3 BV nicht erfüllen. Wie dem auch sei: Die wesentlichen Datenkategorien, Bearbeitungszwecke und Eingriffsvoraussetzungen müssen aufgrund des Legalitätsprinzips auf der Ebene des Gesetzes bestimmt sein und nicht einer Verordnung überlassen werden. Die Piratenpartei Schweiz lehnt deshalb - und aus Prinzip - eine weitreichende Kompetenz des BAKOM zum verdeckten Profiling natürlicher Personen und zur Verarbeitung biometrischer Identifikationsdaten gänzlich ab. Der für die Cybersicherheit notwendige Austausch technischer Informationen, "Indicators of Compromise" und vergleichbarer nicht personenbezogener Daten soll demgegenüber ausdrücklich möglich bleiben. Absatz 5 ermöglicht über die Verweisung auf Art. 13 und 13b auch die Bekanntgabe dieser Daten an ausländische Behörden. Diese Möglichkeit ist für besonders schützenswerte Personendaten und Profilingresultate zu streichen. Wenn bereits die Notwendigkeit der zugrunde liegenden Eingriffe nur für wenige Ausnahmefälle begründet werden kann, ist eine zusätzliche Weitergabe dieser hochsensiblen Daten ins Ausland nicht zu rechtfertigen.
Anhang	

Rückmeldung zu: Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit: Fragebogen zur Vernehmlassungsvorlage

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Keine Rückmeldung
Begründung	--
Anhang	

Detaillierte Stellungnahme

Titel	Frage 1
Antwortoption	Rückmeldung eingeben
Anpassungen / Gegenvorschlag	--
Begründung	Wir begrüssen ein solches Mitbenutzungsrecht. Bestehende passive Infrastrukturen sollten effizient genutzt werden können, sofern Sicherheit, technische Zumutbarkeit und faire Bedingungen gewährleistet sind. Dies kann den Netzausbau beschleunigen und unnötige Parallelbauten vermeiden.
Anhang	

Titel	Frage 2
Antwortoption	Rückmeldung eingeben
Anpassungen / Gegenvorschlag	--
Begründung	Wir begrüssen auch eine gegenseitige Mitbenutzung. Gleiche Rechte für alle beteiligten Netzbetreiber schaffen faire Bedingungen und ermöglichen eine effizientere Nutzung bestehender Infrastruktur, sofern der jeweilige Hauptdienst nicht beeinträchtigt wird.
Anhang	