



Bern, 27. Mai 2026

Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit

Erläuternder Bericht
zur Eröffnung
des Vernehmlassungsverfahrens



Übersicht

Die Sicherheit der Fernmeldeinfrastrukturen hat in den vergangenen Jahren auf allen Ebenen stark an Bedeutung gewonnen. Sie ist ein zentraler Faktor für den schweizerischen Wirtschaftsstandort sowie für die Sicherheit der Bevölkerung im digitalen Raum. Der Schutz vor Cyberbedrohungen ist deshalb zu einer unverzichtbaren Aufgabe des Bundes geworden, gerade auch im Lichte einer möglichen Zuspitzung der aktuellen geopolitischen Lage. Die vorliegende Revision des Fernmeldegesetzes vom 30. April 1997¹ (FMG) trägt dieser Entwicklung Rechnung und zielt darauf ab, einen ausreichenden Schutz der Benutzerinnen und Benutzer sowie der Fernmeldeinfrastrukturen vor diesen Bedrohungen zu gewährleisten. Schliesslich soll im Zuge der vorliegenden Vernehmlassung geklärt werden, ob Vorgaben zur Mitbenutzung passiver Infrastrukturen den Infrastrukturausbau im Fernmeldebereich begünstigen könnten und auch eine erweiterte Datengrundlage geschaffen werden, um einen effizienten Vollzug des Fernmelderechts zu gewährleisten.

Ausgangslage

Das FMG wurde aufgrund der rasanten technischen Entwicklung im Jahr 2019 angepasst. Der technologische Fortschritt hat seither nichts an Dynamik eingebüsst. Durch die neuen Möglichkeiten sind auch die Sicherheitsrisiken gestiegen. So ist der Schutz vor Cyberbedrohungen gerade auch im Lichte der aktuellen geopolitischen Lage von zentraler Bedeutung. Der Bundesrat erachtet daher zusätzliche Massnahmen für den Fall einer Zuspitzung der geopolitischen Situation als unerlässlich. Es braucht Vorschriften, um die Sicherheit von kritischen Fernmeldeinfrastrukturen wie auch der Notkommunikation zu erhöhen und gleichzeitig das Abhängigkeitsrisiko von einzelnen Akteuren und Staaten zu verringern. Nebst einer erhöhten Resilienz der Infrastrukturen soll auch der Schutz der Konsumentinnen und Konsumenten bei der Nutzung von Fernmeldediensten erhöht werden.

Darüber hinaus ist zu berücksichtigen, dass die in den Fernmeldenetzen verwendeten Kupferdoppelader-Metalleitungen in absehbarer Zeit das Ende ihres Lebenszyklus erreichen und ersetzt werden müssen. Dies erfordert ebenfalls eine Anpassung des geltende Rechtsrahmens. Für einen wirksameren Vollzug der Fernmeldegesetzgebung drängt sich im Weiteren auch die Verbesserung der Datengrundlagen über den relevanten Markt auf.

Inhalt der Vorlage

Die Vorlage hat zum Ziel, die Fernmeldeinfrastrukturen in der Schweiz und die darüber erbrachten Dienste sicherer zu gestalten. Dazu werden Massnahmen zur Resilienz der Fernmeldeinfrastrukturen und der Notkommunikation vorgeschlagen. Zum einen soll die Sicherheit der Fernmeldeinfrastruktur erhöht werden. Zu diesem Zweck soll der Bundesrat hinsichtlich einer möglichen Zuspitzung der geopolitischen Lage bei Bedarf geeignete Massnahmen zum Schutz der Fernmeldeinfrastrukturen ergreifen können. Zudem soll künftig die Verfügbarkeit der Notkommunikation durch die Einführung einer Form von Systemführerschaft verbessert werden. Um das Frequenzspektrum vor neuen Störungsphänomenen und Behinderungen des Fernmeldeverkehrs besser zu schützen, sollen sodann im Bereich der Fernmeldeanlagen und der elektrischen Geräte

¹ SR 784.10

Anpassungen der geltenden gesetzlichen Grundlagen vorgenommen werden. Zum anderen soll auch die Sicherheit im Umgang mit Fernmeldediensten für Konsumentinnen und Konsumenten verbessert werden. Hierzu sollen zusätzliche Sperrmöglichkeiten bei missbräuchlich verwendeten schweizerischen Rufnummern oder Domain-Namen sowie erweiterte Informations- und Unterstützungsangebote den Konsumenten- und Jugendschutz verbessern. Darüber hinaus sollen die notwendigen Datenerhebungsgrundlagen geschaffen werden, die eine verbesserten Abbildung der relevanten Marktakteure im Fernmeldebereich ermöglichen.

Schliesslich soll im Rahmen der vorliegenden Vernehmlassungsvorlage geklärt werden, ob zusätzliche Massnahmen den Um- und Ausbau der Fernmeldenetze beschleunigen können.

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Ausgangslage | 6 |
| 1.1 | Handlungsbedarf und Ziele..... | 6 |
| 1.1.1 | Sicherheit | 6 |
| 1.1.2 | Infrastrukturausbau | 7 |
| 1.1.3 | Datengrundlagen | 7 |
| 1.2 | Geprüfte Alternativen und gewählte Lösung..... | 7 |
| 1.2.1 | Sicherheit | 7 |
| 1.2.2 | Infrastrukturausbau | 10 |
| 1.2.3 | Datengrundlagen | 12 |
| 1.3 | Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates..... | 13 |
| 1.4 | Erledigung parlamentarischer Vorstösse..... | 13 |
| 2 | Rechtsvergleich, insbesondere mit dem europäischen Recht . | 15 |
| 2.1 | Sicherheit..... | 15 |
| 2.2 | Infrastrukturausbau..... | 18 |
| 2.3 | Datengrundlagen..... | 18 |
| 3 | Grundzüge der Vorlage | 20 |
| 3.1 | Die beantragte Neuregelung..... | 20 |
| 3.1.1 | Sicherheit | 20 |
| 3.1.2 | Infrastrukturausbau | 20 |
| 3.1.3 | Datengrundlagen | 21 |
| 3.2 | Umsetzungsfragen..... | 21 |
| 4 | Erläuterungen zu einzelnen Artikeln | 22 |
| 4.1 | Fernmeldegesetz (FMG)..... | 22 |
| 4.2 | Durch das Bundesgesetz über die Förderung des Ausbaus von Breitbandinfrastrukturen (BBFG) vorgeschlagene Änderungen des FMG..... | 69 |
| 4.3 | Änderung eines anderen Erlasses: Bundesgesetz betreffend die elektrischen Schwach- und Starkstromanlagen (Elektrizitätsgesetz, EleG)..... | 70 |
| 5 | Auswirkungen | 71 |
| 5.1 | Auswirkungen auf den Bund..... | 71 |
| 5.2 | Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete..... | 71 |
| 5.3 | Auswirkungen auf die Volkswirtschaft..... | 71 |
| 5.3.1 | Sicherheit | 71 |
| 5.3.2 | Infrastrukturausbau | 75 |
| 5.3.3 | Datengrundlagen | 76 |
| 5.4 | Auswirkungen auf die Gesellschaft..... | 77 |
| 5.5 | Andere Auswirkungen..... | 77 |
| 6 | Rechtliche Aspekte | 78 |
| 6.1 | Verfassungsmässigkeit..... | 78 |
| 6.2 | Vereinbarkeit mit internationalen Verpflichtungen der Schweiz..... | 79 |
| 6.3 | Erlassform..... | 80 |
| 6.4 | Unterstellung unter die Ausgabenbremse..... | 80 |

| | | |
|----------|---|-----------|
| 6.5 | Delegation von Rechtsetzungsbefugnissen | 80 |
| 6.6 | Datenschutz | 81 |
| 7 | Abkürzungsverzeichnis | 83 |
| 8 | Literaturverzeichnis | 86 |

Erläuternder Bericht

1 Ausgangslage

1.1 Handlungsbedarf und Ziele

Die Vernehmlassungsvorlage beabsichtigt die Anpassung der fernmelderechtlichen Grundlagen in folgenden Bereichen:

1.1.1 Sicherheit

Die aktuelle geopolitische Lage führt auch in der Telekommunikation zu einem erhöhten Sicherheitsbedürfnis. Technologische Abhängigkeiten können von staatlichen und staatsnahen Akteuren instrumentalisiert werden, um politischen oder wirtschaftlichen Druck auszuüben, kritische Infrastrukturen zu sabotieren oder strategische Informationen abzuschöpfen. Die zunehmende Vernetzung und Digitalisierung erhöhen die Verwundbarkeit gegenüber hybriden Bedrohungen, bei denen technologische Mittel zur Destabilisierung, Erpressung oder gezielten Einflussnahme eingesetzt werden. Eine resiliente und diversifizierte Fernmeldeinfrastruktur ist daher heutzutage zentral für die Handlungsfähigkeit von Staat, Wirtschaft und Gesellschaft.

Das Parlament hat in diesem Zusammenhang verschiedene Vorstösse überwiesen, die von einem Handlungsbedarf für mehr Sicherheit für Fernmeldeinfrastrukturen und -dienste ausgehen. So verlangt insbesondere das Postulat Pult (20.3984) *«Digitale Infrastruktur. Geopolitische Risiken minimieren»* eine Analyse vom Bundesrat, wie geopolitische Risiken beim Ausbau und der Weiterentwicklung von digitalen Infrastrukturen wie 5G minimiert werden können. In seinem Bericht dazu hat der Bundesrat² aufgezeigt, dass es nach dem Vorbild der sogenannten *«5G-Toolbox»* der Europäischen Union (EU)³ und anderer Regulierungsvorhaben, im Fernmeldegesetz (FMG) neue Massnahmen zur Cyberresilienz braucht. Gestützt darauf will er technische Sicherheitsmassnahmen für den Fall einer Zuspitzung der geopolitischen Lage vorsehen, Vorschriften für risikobehaftete Infrastrukturen erlassen und die Abhängigkeit von gewissen Staaten und Herstellern durch die Vorgabe einer Mehrlieferantenstrategie verringern.

Auch unabhängig der geopolitischen Lage ist die Resilienz und technische Sicherheit der Fernmeldeinfrastruktur in der Schweiz zentral. Deren Verwundbarkeit trat in den vergangenen Jahren konkret 2020 und 2021 zu Tage, als diverse Ausfälle im Netz von Swisscom die Erreichbarkeit von Notrufzentralen eingeschränkt haben. Die in diesem Zusammenhang eingereichte Motion der KVF-S (21.3000) *«Systemführerschaft für die Abwicklung von Notrufen»* verlangt die Schaffung gesetzlicher Grundlagen für die Einführung einer technischen Systemführerschaft. Dadurch soll die lückenlose und qualitativ einwandfreie Abwicklung der Notrufe sichergestellt werden.

Die Sicherheit soll aber nicht nur bezüglich der Fernmeldeinfrastrukturen an sich erhöht werden, sondern auch für die Konsumentinnen und Konsumenten. So werden insbesondere in Erfüllung der Motion Gugger (20.3374) *«Unter 16-Jährige wirksam vor pornografischen Inhalten auf dem Internet schützen. #banporn4kids#»* Massnahmen für einen verbesserten Jugendschutz vorgeschlagen. Daneben zeigen das Postulat Maret

Anmerkung: Die Quellenverweise werden im Literaturverzeichnis am Ende des Dokumentes aufgeführt.

² Bundesrat (2023a)

³ EU (2020)

(24.3632) «*Unerwünschte Anrufe. Braucht es neue Massnahmen?*» wie auch die Motionen Seiler-Graf (24.4392) «*Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Rufnummern*» sowie Götte (24.4393) «*Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Domains!*» einen Handlungsbedarf zur Stärkung des Konsumentenschutzes auf. Die vorgeschlagenen Bestimmungen und neuen Kompetenzen des Bundesamtes für Polizei (fedpol) in Zusammenarbeit mit dem Bundesamt für Cybersicherheit (BACS) sollen zur Eindämmung der missbräuchlichen Verwendung von schweizerischen Telefonnummern oder Domain-Namen sowie von missbräuchlichen Anrufen im Allgemeinen beitragen.

1.1.2 Infrastrukturausbau

Neben den genannten, auf Sicherheitsaspekten beruhenden Vorschlägen, soll im Rahmen der Vernehmlassungsvorlage geklärt werden, ob der Infrastrukturausbau mit spezifischen Massnahmen weiter unterstützt werden könnte (vgl. Kapitel [1.2.2](#)). Dies insbesondere deshalb, weil die bisher im Anschlussbereich der Fernmeldenetze verwendeten Kupferdoppelader-Metalleitungen in absehbarer Zeit das Ende ihres Lebenszyklus erreichen und ersetzt werden müssen.

Der geltende Rechtsrahmen soll ebenfalls wo nötig angepasst werden, weil die Signalübertragung über Kupferdoppeladern zunehmend an Relevanz verliert. Zudem soll die Vernehmlassung aufzeigen, ob die Mitbenutzung passiver Infrastrukturen einen Beitrag zum effizienteren Ausbau der Glasfaserleitungen leisten kann und ob weitere Massnahmen dazu erforderlich sind.

1.1.3 Datengrundlagen

Zurzeit werden nur Anbieterinnen registriert, die beim Bundesamt für Kommunikation (BAKOM) Ressourcen beziehen. Dies führt im Vollzug und der Evaluation des Fernmeldegesetzes zu einer mangelhaften Situation. Eine effektive Aufsicht über alle Anbieterinnen und weiteren Akteuren, die dem Fernmelderecht unterliegen, kann dadurch nur eingeschränkt gewährleistet werden. Eine weitergehende Registrierungsmöglichkeit des BAKOM soll die Mängel beheben und zur Schaffung einer umfassenden Datengrundlage beitragen. Im Zusammenhang mit der Datenbearbeitung und -weitergabe enthält die Vorlage auch Anpassungen, die sich aus der Revision des Bundesgesetzes vom 25. September 2020⁴ über den Datenschutz (Datenschutzgesetz, DSG) ergeben.

1.2 Geprüfte Alternativen und gewählte Lösung

1.2.1 Sicherheit

Infrastrukturen

Zur Erhöhung der Sicherheit der Fernmeldeinfrastrukturen in der Schweiz (vgl. Art. 48b und 48c) wurden lediglich diejenigen Massnahmen geprüft und berücksichtigt, die der Bundesrat in seinem Bericht vom 15. Dezember 2023⁵ in Erfüllung des Postulates Pult (20.3984) – welches die Minimierung der geopolitischen Risiken bei der Weiterentwick-

⁴ SR 235.1

⁵ Bundesrat (2023a)

lung von Infrastrukturen wie 5G fordert – vorgeschlagen hat. Regulierungsbedarf besteht auch, weil der freie Markt einige der grundlegenden Cyberbedrohungen für Fernmeldeinfrastrukturen nicht zu beheben vermag.⁶

Die im Bereich der Fernmeldeanlagen notwendig gewordenen Sicherheitsmassnahmen sollen mit der technischen Evolution Schritt halten. Dabei sollen insbesondere die Begrifflichkeiten in den Artikeln 32a, 32b und 34 erweitert werden, um neuen technischen Phänomenen Rechnung tragen zu können. Alternativen bestehen nicht, da gezielt bestehende Lücken in der Gesetzgebung geschlossen werden sollen.

Des Weiteren soll eine Verpflichtung zur Aushändigung aller relevanten technischen Informationen (vgl. Art. 34a Abs. 1) wie auch eine automatisierte optische Erfassung von Fahrzeugen zur Identifikation von Störsignalen (vgl. Art. 34a Abs. 2 und 3) eingeführt werden. Auch in diesen Bereichen sollen gezielt bestehende Lücken in der Gesetzgebung geschlossen werden.

Dasselbe gilt für die Ergänzung und (Wieder-)Einführung einer Sanktionsmöglichkeit betreffend die Störung des Fernmeldeverkehrs und des Rundfunks (vgl. Art. 52 Abs. 1 Bst. g und j). Im Zusammenhang mit der Kompetenzdelegation an den Bundesrat und an das BAKOM im Bereich der elektromagnetischen Verträglichkeit (vgl. Art. 3, 21 und 26b des Bundesgesetzes vom 24. Juni 1902⁷ betreffend die elektrischen Schwach- und Starkstromanlagen (Elektrizitätsgesetz; EleG) hat das Bundesamt für Justiz (BJ) anlässlich der letzten Revision bemängelt, dass es an einer Kompetenzregelung zugunsten des BAKOM im Bereich der elektromagnetischen Verträglichkeit fehle. Diesem Ansinnen kann mit den vorliegenden Anpassungen entsprochen werden.

Notkommunikationssystem

Die Anbieterinnen des öffentlichen Telefondienstes sollen neu auch eine minimale Rückfallebene sicherstellen sowie technische Anforderungen aus Systemaufgaben der Notkommunikation erfüllen (vgl. Art. 20 Abs. 2 und Art. 20a Abs. 2). Die Systemaufgaben sollen namentlich den Betrieb eines hochverfügbaren Notkommunikationsnetzes (*Emergency Services IP Network*, ESInet) durch eine oder redundant durch zwei Anbieterinnen, die Erbringung des Dienstes Standortidentifikation sowie den Betrieb einer zentralen Koordinationsstelle für akute Notkommunikationsanliegen umfassen (vgl. Art. 20a). Werden diese Systemaufgaben nicht bereits sichergestellt, so soll das BAKOM eine oder mehrere Anbieterinnen dazu bezeichnen können (vgl. Art. 20b). Nebst der Kostenregelung (vgl. Art. 20c) enthält die Vorlage auch die Vorgaben für eine Plattform, die End-zu-End-Tests ermöglicht (vgl. Art. 20d), sowie zum Schutz der Integrität der Notkommunikation (vgl. Art. 20e).

Eine weitergehende Systemführerschaft mit umfassendem Weisungsrecht wurde hingegen verworfen. Sie hätte unerwünschte wettbewerbliche Implikationen für andere Anbieterinnen von Fernmeldediensten, da deren Handlungsspielraum stärker eingeschränkt würde, beispielsweise in Bezug auf Ressourcenplanung und Technologiewahl. Ausserdem entstünden bei der Herstellung echter Redundanz durch den Beizug einer Zweitanbieterin Probleme bezüglich beschaffungsrechtlicher Vorgaben, falls die Mandatierung der Zweitanbieterin durch eine Systemführerin und nicht durch das BAKOM erfolgen würde. Ebenfalls verworfen wurde die Idee einer bestimmenden Rolle des BAKOM im Notrufsystem. Demnach hätte das BAKOM Vorgaben insbesondere

⁶ Schwaab (2023)

⁷ SR 734.0

auf Basis internationaler Standards machen können, ohne dabei Anwendersicht auf operative Prozesse bei Anbieterinnen, Geräteherstellern und Zentralen der Notdienste zu haben. Im BAKOM sind nur einzelne Spezialisten für Notkommunikation tätig. Eine Systemführerschaft oder das Führen von Response Teams im BAKOM bei akuten Gefährdungen erscheint deshalb weder möglich noch zweckmässig. Weiter wurde auch die Vereinheitlichung der verschiedenen Telefonnummern für Notdienste auf die 112 geprüft. Einzelne Länder⁸ kennen eine einheitliche Nummer. Damit ginge potenziell eine Reduktion der Zentralen der Notdienste einher. Eine solche Vereinheitlichung würde Anpassungen auf Gesetzesstufe erfordern und könnte zur Reduktion von Kosten und Komplexität in der Notkommunikation führen. Für die Informationsvermittlung zu Notrufnummern an die Bevölkerung wäre eine solche Vereinheitlichung auf eine Nummer möglicherweise ebenfalls nützlich. Gleichzeitig ist es dem föderalen System der Schweiz inhärent, dass solche Massnahmen auf Stufe Bund nur bei entsprechendem Bedarf beziehungsweise auf Wunsch der Kantone realisiert würden. Diese betreiben die Alarmzentralen und deren Vertreter in der Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS), Polizeitechnik und -informatik Schweiz (PTI), Feuerwehr Koordination Schweiz (FKS) und Interverband für Rettungswesen (IVR)⁹ erachten derzeit eine verstärkte Kommunikation über eine einzelne Notrufnummer (112) als nachteilig, weshalb auch diese Massnahme verworfen wurde. Abschliessend wurde geprüft, ob eine vereinfachte oder kostengünstigere Regelung für die kleinen und mittleren Anbieterinnen denkbar wäre. Bei den Regelungen, welche die Kommunikation in Notfällen sicherstellen soll, erscheinen Differenzierungen nicht sinnvoll. Alle Bürgerinnen und Bürger sollten unabhängig der von ihnen gewählten Anbieterin eine Notkommunikation mit vollem Funktionsumfang absetzen können. Zur Wahrnehmung der Systemaufgaben (vgl. Art. 20a) wird hingegen ein zumindest mittelgrosses Unternehmen mandatiert werden müssen. Die Wahrnehmung dieser Aufgaben setzt ein bestimmtes Mass an Ressourcen und operativer Erfahrung bei Netzleistungen voraus.

Jugend- und Konsumentenschutz

Zur Verbesserung des Konsumentenschutzes sind drei neue Massnahmen vorgesehen. Einerseits sollen die Anbieterinnen von Internetzugängen verpflichtet werden, ihre Kundinnen und Kunden über die Möglichkeiten im Bereich des Kinder- und Jugendschutzes zu beraten und ihnen Instrumente anzubieten, mit denen Kinder und Jugendliche wirksam vor pornografischen Inhalten geschützt werden können. Die Aufklärung umfasst die Beratung im Shop, online oder auch telefonisch (vgl. Art. 46a). Durch diese Massnahmen wird die Motion Gugger (20.3374) in der durch den Ständerat geänderten Form umgesetzt.

Weiter soll die heute geltende Sperrpflicht nach Artikel 6a künftig nicht mehr nur bei Prepaid-Angeboten Geltung haben. Unter missbräuchlicher Verwendung einer Identität oder von Zahlungsmitteln können auch *Postpaid*-Angebote bezogen werden. Die Möglichkeit, einen Anschluss sperren zu lassen, soll daher für alle Angebote (Mobilfunk oder Festnetz, *Post*- oder *Prepaid*) erweitert werden. Zudem soll die Möglichkeit, einen Anschluss zu sperren, nicht nur dann bestehen, wenn die Identifikation des Teilnehmers nicht oder nur ungenügend stattgefunden hat. Dies soll auch dann möglich sein, wenn der Verdacht besteht, dass eine Nummer auf betrügerische oder kriminelle Art verwendet wird. Der entsprechende Hinweis dazu muss von einer anerkannten Stelle

⁸ z. B. Finnland; *Emergency Response Centre Agency (2022)*

⁹ *KKPKS, PTI, FKS und IVR (2024)*

kommen (analog Art. 15 Abs. 3 der Verordnung vom 5. November 2014¹⁰ über Internet-Domains, VID).

Zum Schutz der Benutzerinnen und Benutzer soll schliesslich eine Sperranordnung geschaffen werden, damit betrügerisch verwendete schweizerische Telefonnummern und Domain-Namen rasch und befristet blockiert werden können. Diese Massnahmen dienen insbesondere der Umsetzung der Motionen Seiler-Graf (24.4392) und Götte (24.4393).

Das BACS ist die Anlaufstelle für Cybervorfälle und -bedrohungen. Es erhält entsprechende Meldungen aus der Bevölkerung oder von Behörden im Sinne von Artikel 73b des Bundesgesetzes vom 18. Dezember 2020¹¹ über die Informationssicherheit (Informationssicherheitsgesetz, ISG) und analysiert diese. Zum Schutz vor Cyberbedrohungen soll das fedpol mit Unterstützung des BACS die Informationen aus diesen Meldungen hinsichtlich eines mutmasslichen Betrugs unter Verwendung schweizerischer Telefonnummern oder Internet-Domains beurteilen. Zu diesem Zweck leitet das BACS entsprechende Informationen an fedpol weiter, damit Letzteres bei Vorliegen eines begründeten Verdachts eine Sperranweisung vornehmen könnte. Bei einem begründeten Verdacht auf einen mutmasslichen Betrug soll fedpol sodann die Anbieterinnen von Fernmeldediensten oder Registerbetreiberinnen einer Internet-Domain darauf hinweisen, die vorläufige und befristete Sperrung der betreffenden Adressierungselemente vorzunehmen. Dadurch können mutmassliche Straftaten verhindert werden. Der Faktor Zeit spielt dabei eine zentrale Rolle. Es braucht Massnahmen, um rasch reagieren zu können. Je länger eine Telefonnummer in Betrieb ist oder ein Domain-Name aufgerufen werden kann, desto höher ist die Wahrscheinlichkeit von weiteren Opfern. Betrüger können bis zu einer Intervention der zuständigen Strafverfolgungsbehörden mit ihrer Nummer oder ihrem Domain-Namen weiterhin kriminelle Aktivitäten betreiben. Eine rasche Handlungsmöglichkeit ist auch aufgrund der schnell fortschreitenden Entwicklung neuer Technologien und der Mobilität von Betrügern und Cyberkriminellen, die in der Regel international aufgestellt sind, angezeigt. Diese schnelle Interventionsmöglichkeit verfolgt einen präventiven Charakter und soll dem eigentlichen Strafverfahren vorgelagert sein. Falls sich der Verdacht eines Betrugs erhärten sollte, wäre nach Ablauf der Sperranordnung ein ordentliches Strafverfahren bei den zuständigen Strafverfolgungsbehörden einzuleiten.

Diese Massnahmen im Bereich des Jugend- und Konsumentenschutz beruhen auf Anliegen aus parlamentarischen Vorstössen. Aus formellen rechtsstaatlichen Gründen wurde die gemäss der Motion Götte (24. 4393) verlangte Umsetzung der Massnahmen auf Verordnungsstufe verworfen. Anstelle dessen wird eine Umsetzung im Rahmen von Artikel 6b auf Gesetzesstufe vorgeschlagen.

1.2.2 Infrastrukturausbau

Die in den Fernmeldeanschlussnetzen verwendeten Kupferdoppelader-Metalleitungen erreichen in absehbarer Zeit das Ende ihres Lebenszyklus und müssen ersetzt werden. Der geltende Rechtsrahmen soll deshalb auch diesem Umstand angepasst werden. Zur Unterstützung des damit verbundenen Infrastrukturausbaus soll das BAKOM technische und administrative Vorschriften zur gebäudeinternen Verkabelung erlassen kön-

¹⁰ SR 784.104.2

¹¹ SR 128

nen und so Standards definieren. Die Vorgaben sollen sich insbesondere an den bestehenden technischen Richtlinien des BAKOM¹² orientieren. Netzbetreiber, die bestehende gebäudeinterne Kabel mitbenutzen wollen, sollen überall dieselben Bedingungen antreffen. Damit soll die Nutzbarkeit für Dritte sichergestellt werden.

Ein allgemeines Mitbenutzungsrecht an passiven physischen Infrastrukturen aller Netzbetreiberinnen wird hingegen nicht aktiv vorgeschlagen. Dies insbesondere, da der Nutzen in einer unter den Inhaberinnen von *Fiber to the Home* (FTTH) -Betreibernummern durchgeführten Umfrage kontrovers beurteilt wurde¹³. Zudem gibt es Beispiele von Mitbenutzung auf freiwilliger Basis und die Mitbenutzung der Anlagen von marktbeherrschenden Anbieterinnen ist im FMG bereits vorgesehen. Im Rahmen der vorliegenden Vernehmlassungsvorlage soll jedoch geklärt werden, ob eine entsprechende Pflicht der Mitbenutzung passiver physischer Infrastrukturen von sektorfremden Netzbetreiberinnen dennoch sinnvoll wäre.

Daneben wurde geprüft, ob eine Pflicht für Hauseigentümerinnen und -eigentümer eingeführt werden kann, bei Neubauten und umfassenden Renovierungen Leerrohre bis zum Netzabschlusspunkt zu verlegen und einen Netzzugangspunkt zu installieren. Mit diesen gebäudeinternen Anlagen könnte der Ausbau von Glasfasernetzen erleichtert werden. Diese Vorgehensweise wird bei Neubauten bereits zu einem grossen Teil berücksichtigt. Die Definition umfassender Renovierungen kann in der Praxis zu Problemen führen. Es wird der Eigenverantwortung der Hauseigentümerinnen und -eigentümer überlassen, ihre Liegenschaften mit zukunftsfähiger Kommunikationstechnologie auszustatten, weshalb eine verpflichtende Massnahme verworfen wurde.

Auch wurde eine Informationspflicht in Betracht gezogen, um die Transparenz im Bereich der Leitungen und Bauarbeiten zu erhöhen. Der Aufbau eines digitalen Informationssystems zur Lage von Versorgungsleitungen durch das BAKOM ist nicht notwendig, da bereits ein Projekt vom Bundesamt für Landestopografie (swisstopo)¹⁴ mit dem Namen «Leitungskataster Schweiz» besteht. Zusätzlich denkbar wäre eine Auskunftspflicht für Netzbetreiberinnen zu laufenden und geplanten Bauarbeiten. Diese könnte potenziell die Koordination von Bauarbeiten fördern. Hierbei ist zu berücksichtigen, dass das Bauwesen grundsätzlich von den Kantonen und Gemeinden geregelt wird. Die erwähnte Umfrage unter den Inhaberinnen von FTTH-Betreibernummern hat gezeigt, dass das Kosten-Nutzen-Verhältnis einer solchen Massnahme umstritten ist. Für geplante Bauarbeiten könnte der genannte Leitungskataster später im Bereich Bauprojekte (Projektierung und Baubewilligung) erweitert werden¹⁵.

Weiter wurde erwogen, die Netzbetreiberinnen zu verpflichten, zumutbaren Anträgen auf Abschluss einer Vereinbarung über die Koordinierung von Bauarbeiten unabhängig von Artikel 75 der Verordnung vom 9. März 2007¹⁶ über Fernmeldedienste (FDV) stattzugeben. Die Massnahme wurde verworfen, weil die Einschätzung in der genannten Umfrage zum Kosten-Nutzen-Verhältnis unklar ausfällt und in vielen Kantonen und Gemeinden¹⁷ Strukturen für eine Koordination von Bauarbeiten bestehen.

¹² BAKOM (2012)

¹³ BAKOM (2024a und b)

¹⁴ swisstopo (2024a)

¹⁵ swisstopo (2024b)

¹⁶ SR 784.101.1

¹⁷ Z. B. in der Stadt Zürich: *Stadt Zürich* (2020)

Um wettbewerblich tendenziell vorteilhafte Kooperationen zu fördern, wurde ebenfalls geklärt, ob bei regulierten Vorleistungen von marktbeherrschenden Anbieterinnen (insbesondere Kabelkanalisationen) im Rahmen von Kooperationsvereinbarungen ein gewisses Abweichen vom Grundsatz der Nichtdiskriminierung und / oder der Kostenorientiertheit gemäss Artikel 11 erlaubt werden sollte. Damit würde in den Kooperationsverhandlungen insbesondere der finanzielle Handlungsspielraum vergrössert. Ein Grossteil, der in der genannten Umfrage befragten Marktteilnehmer, sieht indes keinen Nutzen in einer derartigen Regelung und die Auswirkungen auf den Ausbau werden mehrheitlich als gering eingeschätzt.

Sodann wurde geprüft, ob die erste Unternehmung, die in einem Gebiet den Ausbau eines FTTH-Netzes meldet, während beispielsweise fünf Jahren ein exklusives Recht zur Erschliessung der Nutzungseinheiten in diesem Gebiet erhalten sollte. Aufgrund der Befristung dieser Massnahme ist der Nutzen bezüglich Investitionssicherheit beschränkt. Gleichzeitig käme eine solche Massnahme an Orten mit mehreren Anschlusstechnologien (z. B. CATV und FTTC), welche potenziell beide von verschiedenen Anbieterinnen auf FTTH aufgerüstet werden, einem temporären Investitionsverbot gleich. Bereits heute sind allein von der Marktführerin Swisscom¹⁸ gut die Hälfte der Haushalte mit FTTH erschlossen und Pläne für den weiteren Ausbau dürften bereits erstellt sein. Ein befristetes exklusives Erschliessungsrecht käme zu spät und wäre potenziell bei der Umsetzung aufgrund möglicher Rechtsverfahren mit Verzögerungen für den Glasfaserausbau verbunden.

Die abschliessende Prüfung bezüglich vereinfachter oder kostengünstigerer Regelung für die kleinen und mittleren Unternehmen nach dem Bundesgesetz vom 29. September 2023¹⁹ über die Entlastung der Unternehmen von Regulierungskosten (UEG) führt zum Schluss, dass es sich bei den technischen Vorschriften zur gebäudeinternen Verkabelung um Massnahmen handelt, welche insbesondere kleineren Anbieterinnen den Markteintritt erleichtern sollen. Eine weitergehende Vereinfachung der vorgeschlagenen Massnahmen ist daher nicht angezeigt.

1.2.3 Datengrundlagen

Das geltende Recht in Bezug auf die Registrierung der auf dem Fernmeldemarkt tätigen Unternehmen hat Lücken gezeigt, die geschlossen werden müssen, da die Behörden andernfalls einige ihrer Aufgaben nicht wahrnehmen können. Zur Behebung dieser Mängel sieht die gewählte Lösung die Erfassung der derzeit nicht registrierten Fernmeldedienst- und Internetzugangsanbieterinnen oder von gewissen Eigentümerinnen sowie Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen vor. Ziel ist, dadurch ein möglichst repräsentatives Bild der relevanten Akteure zu erhalten. Nur mit einer genauen Kenntnis der Marktteilnehmer ist es möglich, jedes Jahr eine Fernmeldestatistik mit zuverlässigen und validen Indikatoren zu erstellen, alle drei Jahre wie vom Gesetzgeber verlangt einen Evaluationsbericht zur Marktsituation zu erarbeiten (vgl. Art. 3a), die Aufsicht über die Einhaltung des Fernmelderechts durchzuführen (vgl. Art. 58) und fundierte regulatorische Entscheidungen zu treffen.

Die für die Registrierung der Marktteilnehmer gewählte Lösung übernimmt die zielführenden Elemente der beiden Optionen, die in der Vergangenheit galten. So war mit der Meldepflicht bis Ende 2020 für die Fernmeldedienstanbieterinnen zwar eine Gebührenpflicht verbunden. Andererseits besass die Meldepflicht aber den Vorteil, dass der Regulator die betroffenen Marktteilnehmer gesamthaft erfassen konnte. Im geltenden

¹⁸ *Swisscom (2025a)*

¹⁹ SR 930.31

Recht ist keine Gebührenpflicht vorgesehen. Aufgrund zu restriktiver Registrierungskriterien sind aber nicht mehr alle relevanten Akteure bekannt, denn es müssen sich nur Marktteilnehmer registrieren lassen, die bestimmte staatlich verwaltete Ressourcen nutzen. Die vorliegend gewählte Lösung umfasst beide oben erwähnten zentralen Aspekte: einerseits die kostenlose Registrierung und andererseits die Möglichkeit, alle für den schweizerischen Markt relevanten Teilnehmer zu erfassen.

1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Vorlage ist weder in der Botschaft vom 24. Januar 2024²⁰ zur Legislaturplanung, noch im Bundesbeschluss vom 6. Juni 2024²¹ über die Legislaturplanung 2023-2027 angekündigt.

Die Teilrevision des FMG ist dennoch angezeigt, da die vorgeschlagenen Massnahmen zur Erfüllung des Ziel 20 des Bundesbeschlusses zur Legislaturplanung 2023-2027²² beitragen. Gemäss diesem Ziel soll der Bund Cyberrisiken antizipieren und wirksame Massnahmen ergreifen, um die Bevölkerung, die Wirtschaft sowie die kritischen Infrastrukturen zu schützen. Mit den vorgeschlagenen Sicherheitsmassnahmen kann diesbezüglich ein wichtiger Beitrag geleistet werden.

Die Nationale Cyberstrategie NCS²³ gegen Cyberbedrohungen wie auch die Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI-Strategie)²⁴, namentlich das Ziel «Sichere und verfügbare digitale Dienstleistungen und Infrastruktur»²⁵, greifen diesen präventiven Ansatz auf. Sie beauftragen den Bundesrat aber zugleich, Cyberrisiken und -verwundbarkeiten zu analysieren und unter Berücksichtigung von Bedürfnissen und Gesetzeslücken notwendige Regelungen vorzuschlagen. Die vorliegende Vernehmlassungsvorlage operationalisiert damit die nationale Resilienzpolitik im Bereich Cyber-, Kommunikations- und Kriseninfrastruktur und trägt zur Umsetzung der Sicherheitspolitischen Strategie sowie der Nationalen SKI-Strategie bei.

1.4 Erledigung parlamentarischer Vorstösse

Mit der Vernehmlassungsvorlage werden die geforderten Sicherheitsanliegen des überwiesenen Postulats Pult (20.3984) «*Digitale Infrastruktur. Geopolitische Risiken minimieren*», der Motion der KVF-S (21.3000) «*Systemführerschaft für die Abwicklung von Notrufen*» umgesetzt. Die Vorlage trägt überdies zur Umsetzung der Anliegen des Postulates Z`Graggen (22.4411) «*Strategie Digitale Souveränität der Schweiz*», der Motion Dittli (23.3002) «*Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz*» sowie den Motionen Juillard (24.3209) und Chappuis (24.3363) «*Für eine souveräne digitale Infrastruktur in der Schweiz im Zeitalter der künstlichen Intelligenz*» bei.

Die vorgeschlagenen Änderungen im Bereich des Konsumenten- und Jugendschutzes erfüllen die in der Motion Gugger (20.3374) «*Unter 16-Jährige wirksam vor pornografischen Inhalten auf dem Internet schützen. #banporn4kids#*», dem Postulat Maret

²⁰ BBI 2024 525

²¹ BBI 2024 1440

²² Artikel 21, https://www.fedlex.admin.ch/eli/fqa/2024/1440/de#art_21

²³ Bundesrat (2023b)

²⁴ Bundesrat (2023c)

²⁵ NCS (2023)

(24.3632) «*Unerwünschte Anrufe. Braucht es neue Massnahmen?*» geäusserten Forderungen. Den Anliegen der Motion Seiler-Graf (24.4392) «*Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Rufnummern*» und der Motion Götte (24.4393) «*Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Domains!*» werden ebenfalls durch die vorgeschlagene Massnahmen Rechnung getragen.

Die thematisch verwandte und gleichzeitig eingereichte Motion Candinas (24.4391) «*Es braucht einen wirksamen Schutz gegen Call-ID-Spoofing von schweizerischen Rufnummern!*» kann gestützt auf die geltenden formell-rechtlichen Bestimmungen im FMG auf Verordnungsstufe umgesetzt werden.

2 Rechtsvergleich, insbesondere mit dem europäischen Recht

2.1 Sicherheit

Infrastrukturen

Die Europäische Union nimmt die Sicherheit ihrer digitalen Netzwerke und Informationssysteme als kritische Infrastrukturen für Wirtschaft und Gesellschaft sehr ernst. Das EU-Recht zielt deshalb auf die Schaffung eines sicheren und resilienten digitalen Ökosystems ab. Dazu werden Sicherheitsanforderungen für die wichtigen Akteure festgelegt, die Zusammenarbeit zwischen den Mitgliedstaaten gefördert und Zertifizierungs-, Überwachungs- und Sanktionsmechanismen eingeführt. Bürgerinnen und Bürger, Unternehmen und Einrichtungen sollen so vor Cyberbedrohungen geschützt und das einwandfreie Funktionieren des digitalen Binnenmarkts sichergestellt werden.

Die gesetzlichen Grundlagen der EU bilden einen umfassenden rechtlichen Rahmen im Bereich der Sicherheit der digitalen Infrastrukturen und sind in drei Kategorien gegliedert: ausschliesslich der Cybersicherheit gewidmete Regelwerke, Rechtsakte, die Bestimmungen zur Cybersicherheit enthalten, und Grundlagen, die auf die Cybersicherheit verweisen. Im Bereich der Sicherheit der Infrastrukturen, der Dienste und der Endgeräte massgeblich sind im Wesentlichen die Bestimmungen der Verordnung (EU) 2019/881 (*Cybersecurity Act, CSA*)²⁶, der Verordnung (EU) 2024/2847 (*Cyber Resilience Act, CRA*)²⁷, der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)²⁸ sowie des EU-Instrumentariums für 5G-Sicherheit («5G-Toolbox»)²⁹.

Das Abkommen zwischen der Schweizerischen Eidgenossenschaft und der EU über die gegenseitige Anerkennung von Konformitätsbewertungen (*Mutual Recognition Agreements - MRA Schweiz–EU*)³⁰ ist ein Instrument zum Abbau technischer Handelshemmnisse bei der Vermarktung zahlreicher Industrieerzeugnisse zwischen der Schweiz und der EU, insbesondere im Sektor Funkanlagen und Telekommunikationsendgeräte (Kapitel 7). Damit der Sektor im MRA verbleiben kann, muss die entsprechende Schweizer Gesetzgebung an diejenige der EU angeglichen werden. Die Richtlinie 2014/53/EU (RED-Richtlinie)³¹ enthält wesentliche Anforderungen an die Cybersicherheit. Diese können von der Kommission durch einen delegierten Rechtsakt aktiviert werden. In diesem werden dann die Produkte festgelegt, die diese zusätzlichen Anforderungen erfüllen müssen. Im Jahr 2021 veröffentlichte die Kommission einen solchen Rechtsakt, mit dem die Cybersicherheitsanforderungen für bestimmte Funkanlagen aktiviert wurden. Diese Bestimmungen wurden in die Verordnung des BAKOM

²⁶ Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. L 151 vom 7.6.2019, S. 15; geändert durch Verordnung (EU) 2025/37, ABl. L, 2025/37, 15.1.2025.

²⁷ Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. L, 2024/2847, 20.11.2024.

²⁸ Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 26.12.2022, S. 80.

²⁹ EU (2020)

³⁰ SR 0.946.526.81

³¹ Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG, ABl. L 153 vom 22.5.2014, S. 62; zuletzt geändert durch Richtlinie (EU) 2024/2839, ABl. L, 2024/2839, 7.11.2024.

vom 26. Mai 2016³² über Fernmeldeanlagen (VFAV) übernommen, um die Gleichwertigkeit der Schweizer Gesetzgebung und den Verbleib des Sektors im MRA zu gewährleisten. Dies, obwohl die EU seit der Einstellung der Verhandlungen über das Rahmenabkommen im Jahr 2021 formal keine Gleichwertigkeitsprüfung mehr durchgeführt hat.

Die RED-Richtlinie³³, an welche die Schweiz ihre Gesetzgebung angeglichen hat, schafft einen Regelungsrahmen für das Bereitstellen auf dem Markt von Funkanlagen, der technische Anforderungen für den Schutz der Privatsphäre, den Schutz personenbezogener Daten und den Schutz vor Betrug umfasst. Die Bestimmungen, die 2022 in die Verordnung vom 25. November 2015³⁴ über Fernmeldeanlagen (FAV) aufgenommen und in der VFAV aktiviert wurden, erhöhen die Cybersicherheit bestimmter drahtloser Geräte (Smartphones, Smartwatches, Fitness-Tracker und drahtlose Spielzeuge), die auf dem Schweizer Markt erhältlich sind. Solche vernetzten Geräte müssen Funktionen aufweisen, die eine Beeinträchtigung der Kommunikationsnetze verhindern, damit deren Resilienz gestärkt wird. Die Bestimmungen der VFAV gelten auch für 5G-Anlagen.

Die USA haben im Mai 2019 die Produkte und Dienstleistungen chinesischer Unternehmen in ihren Telekommunikationssystemen verboten. Dieses Verbot wurde 2022 auf alle chinesischen Telekommunikations- und Videoüberwachungsprodukte ausgeweitet. Die Gründe für das Verbot dürften neben dem Spionageverdacht auch Überlegungen betreffend die Dominanz chinesischer Unternehmen auf dem Markt für 5G-Technologie und den Rückstand der US-Unternehmen in diesem Bereich beinhalten. Andere Länder sind dem Beispiel der USA gefolgt, unter anderem Kanada, das Vereinigte Königreich, Japan und Australien.

Notkommunikation

Im Bereich der Notkommunikation wird bei der aufwändigsten Systemaufgabe, der Erstellung eines ESInet, auf einen internationalen Standard von ETSI³⁵ abgestellt. Gemäss McBride³⁶ haben verschiedene andere europäische Länder wie Nordmazedonien, Österreich, Portugal und Rumänien Teile davon bereits umgesetzt. Bulgarien, Estland, Litauen und Schweden verfolgen entsprechende Projekte. Auch die National Emergency Number Association (NENA)³⁷, die US-amerikanische Standardisierungsbehörde zu Notkommunikation, ist in diesem Bereich aktiv.

Jugend- und Konsumentenschutz

Betreffend Jugendschutz gibt es nach derzeitigem Kenntnisstand in den neuen Leitlinien der EU-Kommission C/2025/5519³⁸ zwar Pflichten für Plattformbetreiber, technische Jugendschutz- und Kontrollwerkzeuge bereitzustellen. Eine darüber hinausgehende gesetzliche Verpflichtung der Internetanbieter zur aktiven Beratung der Erziehungsberechtigten ist jedoch im EU-Recht nicht normiert. Eine solche Regelung liegt

³² SR 784.101.21

³³ Siehe Fussnote 31.

³⁴ SR 784.101.2

³⁵ ETSI (2023)

³⁶ McBride (2024)

³⁷ NENA (2025)

³⁸ Leitlinien C/2025/5519 für Massnahmen zur Gewährleistung eines hohen Masses an Privatsphäre, Sicherheit und Schutz von Minderjährigen im Internet gemäss Artikel 28 Absatz 4 der Verordnung (EU) 2022/2065, ABl. C, 10.10.2025.

im Ermessensspielraum der Mitgliedstaaten. Im Bereich der Telefonnummer- und Domainsperrung gibt es auf Ebene des Rechts der Europäischen Union (EU-Recht) derzeit keine Rechtsnorm, die Behörden bereits bei Vorliegen eines begründeten Tatverdachts zur Anordnung solcher Eingriffe berechtigt. Der nachfolgende Quervergleich mit der Rechtsanwendung in den an die Schweiz grenzenden Ländern ist daher von besonderem Interesse.

Die deutsche Bundesnetzagentur (BNetzA) hat die Befugnis, bei Nichterfüllung gesetzlicher oder behördlicher Verpflichtungen die mutmasslich rechtswidrig genutzte Rufnummer zu entziehen. Darüber hinaus kann die BNetzA dem Netzbetreiber, in dessen Netz die Rufnummer geschaltet ist, die Abschaltung der Rufnummer anordnen. Es ist davon auszugehen, dass die BNetzA bei einem dringenden und stichhaltig begründeten Tatverdacht der ermittelnden Behörde, die Abschaltung der Rufnummer anordnen könnte, auch wenn noch keine rechtskräftige Verurteilung vorliegt. Die Beschwerdeordnung³⁹ der BNetzA legt den Fokus auf die Ermittlung von Tatsachen durch die BNetzA selbst. Die „gesicherte Kenntnis“ wird hierbei durch die Summe der vorliegenden Beschwerden und Beweismittel generiert, was ein sofortiges Eingreifen (Abschaltung) zur Gefahrenabwehr ermöglicht, ohne dass ein strafrechtliches Urteil abgewartet werden muss. Gemäss Pressemitteilung der BNetzA⁴⁰ wurden allein im Jahr 2024 insgesamt rund 6.500 Rufnummern abgeschaltet. Die hohe Zahl jährlicher Abschaltungen lassen gar nicht zu, dass zuvor eine rechtskräftige Verurteilung vorliegen müsste. Hervorzuheben ist zudem, dass die Formulierung «bei gesicherter Kenntnis von der rechtswidrigen Nutzung einer Rufnummer (...)» höhere Anforderungen an die Beweislast stellt als ein begründeter Verdacht. Die BNetzA muss aufgrund von Tatsachen davon überzeugt sein, dass eine rechtswidrige Nutzung vorliegt.

Die französische *Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse* (ARCEP) kann die Sperrung von Telefonnummern im Sinne einer Sanktionsmassnahme nach förmlicher Aufforderung und bei festgestellter Nichteinhaltung der Vorschriften zur Nutzung von Nummerierungsressourcen anordnen. Typischerweise wird die Betreiberin oder der Benutzer förmlich aufgefordert («*Mise en demeure*») den Verstoss innerhalb der festgelegten Frist zu beheben. Wenn der Verstoss nach Ablauf der Frist weiterhin besteht, kann die ARCEP die Betreiber anordnen, die Nummer zu sperren.

Die italienische *Autorità per le Garanzie nelle Comunicazioni* (AGCOM) ist eine Regulierungsbehörde mit umfassenden Kontroll- und Sanktionsmöglichkeiten im Kommunikationssektor. Ihre Rechtsgrundlage ist der *Codice delle Comunicazioni Elettroniche* (Elektronischer Kommunikationskodex). Bei festgestelltem Missbrauch oder Nichteinhaltung der Vorschriften bezüglich der Nutzung von Nummerierungsressourcen kann die AGCOM Sanktionen verhängen. Das Verfahren sieht in der Regel eine förmliche Beanstandung vor, gefolgt von der Möglichkeit der Deaktivierung der Telefonnummer, wenn der rechtswidrige Zustand nicht fristgerecht beseitigt wird. Italien hat auch spezifische Regelungen zur Bekämpfung von Telekommunikationsbetrug, bei denen die Abschaltung der Nummer als direkte Konsequenz vorgesehen ist. Die Anordnung erfolgt auf Basis eines Verwaltungsaktes. Auf der Grundlage des *Codice di Procedura Penale* (Strafprozessordnung) kann die Staatsanwaltschaft oder der *Giudice per le Indagini Preliminari* (Richter für die Vorermittlungen) bei einem dringenden und schwerwiegenden Tatverdacht (z.B. im Zusammenhang mit Terrorismus, Drogenhandel oder schwe-

³⁹ BNetzA (2022)

⁴⁰ BNetzA (2025)

rem Betrug) die vorsorgliche Sicherstellung und Unterbrechung von Kommunikationsmitteln anordnen. Dies dient dazu, die Fortsetzung der kriminellen Tätigkeit zu unterbinden, bevor es zu einer Anklage oder Verurteilung kommt.

Die österreichische Rundfunk und Telekom Regulierungs-GmbH (RTR) besitzt umfassende verwaltungsstrafrechtliche Befugnisse und Kompetenzen zur Durchsetzung des Telekommunikationsrechts. Ihre Rechtsgrundlage ist das Telekommunikationsgesetz (TKG 2021), insbesondere die Paragraphen, welche die Nutzung von Nummerierungsressourcen regeln und die Verwaltungsstrafbestimmungen festlegen. In der Praxis kann die RTR bei festgestelltem Missbrauch von Telefonnummern (z.B. bei unerlaubter Werbung, illegalen Abzock-Maschen oder Massenbelästigung) Massnahmen zur Beseitigung des rechtswidrigen Zustands anordnen. Dies kann die Verpflichtung des Betreibers umfassen, die Nutzung der Telefonnummer zu unterbinden, was faktisch einer Sperrung gleichkommt. Es ist dazu kein zivil- oder strafrechtliches Urteil erforderlich. Bei einem dringenden Tatverdacht und wenn bereits ein Strafverfahren läuft, sind die Gerichte und Staatsanwaltschaften zuständig. Hier ist die Rechtsgrundlage die Strafprozessordnung. Bei einem dringenden Tatverdacht für schwere Straftaten kann die Staatsanwaltschaft oder das Gericht gemäss der Strafprozessordnung Überwachungs- oder Sicherungsmassnahmen anordnen. Die vorübergehende Abschaltung einer Telefonnummer als Massnahme zur Gefahrenabwehr oder Unterbindung weiterer Straftaten muss richterlich bewilligt werden und dient als Sicherstellung.

Die Beispiele aus Deutschland, Frankreich, Italien und Österreich zeigen, dass es in den angrenzenden Nachbarstaaten der Schweiz keine gleichlautende explizite Regelung gibt, die es den Ermittlungsbehörden erlaubt, Nummern bereits bei begründetem Tatverdacht sperren zu lassen. Gleichzeitig wird aber deutlich, dass kein rechtskräftiges Urteil als zwingende Voraussetzung für die Sperrung erforderlich ist. Die Sperrung erfolgt entweder als Verwaltungssanktion durch die Regulierungsbehörde (auf Basis einer gesicherten Kenntnis von der Rechtswidrigkeit) oder als strafprozessuale Sicherungsmassnahme (vor einer rechtskräftigen Verurteilung) auf Anordnung der Justizbehörden (bei dringendem Tatverdacht).

2.2 Infrastrukturausbau

Mit dem Vorschlag, lediglich Vorschriften zur gebäudeinternen Verkabelung zu erlassen, geht die Schweiz im Bereich passive Infrastruktur deutlich weniger weit als die EU. Verschiedene der im Kapitel [1.2.2](#) aufgeführten und verworfenen Handlungsalternativen entstammen der Verordnung (EU) 2024/1309 (*Gigabit Infrastructure Act*, GIA)⁴¹, einem inzwischen in Kraft getretenen EU-Rechtsakt zur Begünstigung des Breitbandausbaus.

2.3 Datengrundlagen

Auf europäischer Ebene existieren gemeinsame Grundsätze und eine Koordination innerhalb der EU. Gemäss der Richtlinie (EU) 2018/1972 (*European Electronic Communications Code*, EECC)⁴² darf ein Mitgliedstaat, der eine Meldepflicht für Unternehmen, die einer Allgemeinenehmigung unterliegen, als gerechtfertigt erachtet, von solchen

⁴¹ Verordnung (EU) 2024/1309 des Europäischen Parlaments und des Rates vom 29. April 2024 über Massnahmen zur Reduzierung der Kosten des Aufbaus von Gigabit-Netzen für die elektronische Kommunikation, zur Änderung der Verordnung (EU) 2015/2120 und zur Aufhebung der Richtlinie 2014/61/EU (Gigabit-Infrastrukturverordnung), ABl. L, 2024/1309, 8.5.2024.

⁴² Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung), ABl. L 321 vom 17.12.2018, S. 36; geändert durch Richtlinie (EU) 2022/2555, ABl. L 333 vom 27.12.2022, S. 80.

Unternehmen lediglich die Übermittlung einer Meldung an die nationale Regulierungsbehörde oder eine andere zuständige Behörde fordern. Die Meldung umfasst nicht mehr als die Erklärung einer natürlichen oder juristischen Person gegenüber der nationalen Regulierungsbehörde oder einer anderen zuständigen Behörde, dass sie die Absicht hat, mit der Bereitstellung elektronischer Kommunikationsnetze oder -dienste zu beginnen, sowie die Mindestangaben, die nötig sind, damit das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und diese Behörde ein Register oder ein Verzeichnis der Anbieter elektronischer Kommunikationsnetze und -dienste führen können. Die Mitgliedstaaten erlegen keine zusätzlichen oder separaten Meldepflichten auf.

Somit fördert der EECC zwar eine harmonisierte und vereinfachte Vorgehensweise, bietet den Mitgliedstaaten aber eine gewisse Flexibilität in der Frage, ob sie eine Meldepflicht auferlegen wollen. Zudem führt und veröffentlicht das GEREK ein Verzeichnis dieser Meldungen in einer Datenbank der Allgemeingenehmigungen mit Angabe unter anderem des Namens des Unternehmens, der bereitgestellten Dienste und der betroffenen Mitgliedstaaten. In der Praxis verlangen alle EU-Mitgliedstaaten eine Meldung, mit Ausnahme Dänemarks, das nie eine Meldepflicht kannte, sowie Frankreichs, das sie 2021 abschaffte. Ausserhalb der EU ist im Vereinigten Königreich nie eine Meldepflicht eingeführt worden. Schliesslich ist es für die meisten europäischen Länder wichtig, über eine genaue Übersicht über die Anbieter elektronischer Kommunikationsnetze oder -dienste zu verfügen - unabhängig von der Art und Weise, wie die Angaben erfasst werden. Dies ermöglicht insbesondere das Führen eines Verzeichnisses und erleichtert so die Marktbeobachtung und -regulierung.

Im Vergleich dazu sieht die Vernehmlassungsvorlage keine Wiedereinführung einer formellen Meldepflicht für alle Anbieterinnen von Fernmeldediensten vor, wie sie bis vor 2021 galt. Wie auf europäischer Ebene wird aber angestrebt, eine möglichst vollständige Übersicht über die Marktteilnehmer zu haben. Zu diesem Zweck soll das BAKOM die Möglichkeit haben, auch Anbieterinnen von Fernmeldediensten, die keine Ressourcen beim BAKOM beziehen (namentlich Internetzugangsanbieterinnen) oder Eigentümerinnen sowie Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen in der Schweiz zu registrieren und von ihnen alle für die Registrierung notwendigen Angaben zu verlangen.

3 Grundzüge der Vorlage

3.1 Die beantragte Neuregelung

Die Vorlage umfasst im Wesentlichen drei Regelungsbereiche:

3.1.1 Sicherheit

Die Sicherheit der Fernmeldeinfrastrukturen und der darüber erbrachten Dienste muss angesichts der instabilen geopolitischen Lage verbessert werden. Daher werden im Bereich der Fernmeldeinfrastrukturen Vorgaben vorgeschlagen, welche die Resilienz und die Sicherheit der Infrastrukturen an sich erhöhen. Zudem soll der Bundesrat bei Sicherheitsrisiken infolge der geopolitischen Situation die notwendigen Massnahmen ergreifen können. Der Sicherheit der Infrastrukturen dienen nicht zuletzt auch Massnahmen im Bereich der Fernmeldeanlagen und der elektrischen Geräte. Hierzu sollen die Bestimmungen für Anlagen präzisiert werden, die im Interesse der Verbrechensverhütung und Verbrechensbekämpfung sowie der öffentlichen Sicherheit von bestimmten Behörden betrieben werden müssen. Überdies soll das BAKOM zur Identifikation von Störungen des Frequenzspektrums im Verkehr Messanlagen mit einer Bildaufnahmefunktion ausstatten können und damit fehlbare Fahrzeuge identifizieren zu können.

Des Weiteren wird auch eine verbesserte Verfügbarkeit der Notkommunikation angestrebt, welche durch die Einführung einer Form von technischer Systemführerschaft erreicht werden soll.

Schliesslich soll auch die Sicherheit für die Konsumentinnen und Konsumenten im Umgang mit Fernmeldediensten erhöht werden. So müssen Anbieterinnen von Fernmeldediensten die Erziehungsberechtigten ausführlicher über technische Mittel zum Jugendschutz im Bereich der Pornographie informieren. Zudem soll die Bekämpfung des Missbrauchs von schweizerischen Telefonnummern und Domain-Namen verstärkt werden.

3.1.2 Infrastrukturausbau

Zum Zwecke eines effizienten Infrastrukturausbaus soll das BAKOM technische und administrative Vorschriften (TAV) zur gebäudeinternen Verkabelung erlassen können und so Standards definieren. Die Vorgaben sollen sich insbesondere an bestehenden freiwilligen technischen Richtlinien des BAKOM⁴³ orientieren. Überdies wird vorgeschlagen, in den allgemeinen Bestimmungen gewisse Eigentümerinnen oder Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen den Anbieterinnen von Fernmeldediensten gleichzustellen, soweit dies für den wirksamen Wettbewerb beim Erbringen von Fernmeldediensten notwendig ist. Insbesondere im Bereich der Inanspruchnahme von Grund und Boden sowie des Zugangs zum Gebäudeeinführungspunkt und der Mitbenutzung gebäudeinterner Anlagen soll damit eine bisherige Gesetzeslücke geschlossen werden können. Die Vorlage enthält keine expliziten Mitbenutzungspflichten von passiver Infrastruktur. Ob eine entsprechende Verpflichtung erforderlich ist, soll im Rahmen der vorliegenden Vernehmlassung dennoch zur Diskussion gestellt werden.

⁴³ BAKOM (2012)

3.1.3 Datengrundlagen

Zu Vollzugs- und Evaluationsaufgaben soll das BAKOM zusätzliche Akteure des schweizerischen Fernmeldemarktes erfassen können. Die geltenden Grundlagen erlauben dem BAKOM einzig die Registrierung von Anbieterinnen von Fernmeldediensten, welche Ressourcen beim BAKOM beziehen. Dadurch verfügen das BAKOM wie auch andere Behörden nur über eine eingeschränkte Übersicht über den schweizerischen Fernmeldemarkt und dessen relevante Teilnehmer. Wichtige Akteure wie Anbieterinnen von Internetzugangsdiensten oder gewisse Betreiberinnen oder Eigentümerinnen von Fernmeldeanlagen können nach geltendem Recht nicht registriert werden. Es ist für den Vollzug und die Evaluation der fernmelderechtlichen Gesetzgebung jedoch zentral, dass entsprechende Marktteilnehmer erfasst werden können. Mit der Schaffung dieser neuen Registrierungsmöglichkeit, soll dieser Mangel behoben werden.

3.2 Umsetzungsfragen

Die vorgesehenen Sicherheitsmassnahmen von Fernmeldeinfrastrukturen und bei geopolitischen Risiken sind aus der «5G-Toolbox» der EU⁴⁴ abgeleitet. Entsprechend sind diese für international tätige Anbieterinnen ohnehin zu berücksichtigen. Zudem basieren diese auf internationalen Standards. Es ist deshalb von einer einfachen Umsetzbarkeit auszugehen.

Im Bereich Notkommunikation wird insbesondere auf Basis von internationalen Standards reguliert. Der Standard zur Erstellung eines ESInet stammt von der Organisation ETSI (vgl. Kapitel 2), welche bei der Standardisierung Branchenvertreter involviert.⁴⁵ Die Massnahme zur minimalen Rückfallebene geht auf das Referenzmodell Notrufe des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation (UVEK) und der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)⁴⁶ zurück. Im betreffenden Projekt war die Branche ebenfalls vertreten.

Die Massnahmen im Bereich des Konsumentenschutzes enthalten keine Vorgaben, welche den Vollzug mittels elektronischer Mittel verhindern oder behindern könnten. Dasselbe gilt auch für die vorgeschlagene Sperrmöglichkeit von Telefonnummern und Domain-Namen. Jedoch sollen die Beratungen den Erziehungsberechtigten in den Verkaufsstellen der Internetanbieter, telefonisch oder per Online-Formular/Chat-Bot angeboten werden. In allen Fällen ist kein Kontakt mit der Behörde notwendig und die Beratungen können in den meisten Fällen über bereits existierende Verkaufskanäle der Anbieterinnen von Internetzugangsdiensten erfolgen.

Bei den Vorschriften zur gebäudeinternen Verkabelung ist von einer einfachen Umsetzbarkeit auszugehen. Die Vorschriften sollen sich an bestehenden technischen Richtlinien des BAKOM⁴⁷ orientieren, welche in einer Branchenarbeitsgruppe erarbeitet wurden. Die Vorschriften werden elektronisch zugänglich gemacht. Bei allfälligen Aufsichtsverfahren wird auf eine möglichst elektronische Abwicklung geachtet.

⁴⁴ EU (2020)

⁴⁵ ETSI (2025)

⁴⁶ UVEK und KKJPD (2022)

⁴⁷ BAKOM (2012)

4 Erläuterungen zu einzelnen Artikeln

4.1 Fernmeldegesetz (FMG)

Ingress

Das Fernmeldewesen stützt sich grundsätzlich auf die umfassende Bundeskompetenz in Artikel 92 der Bundesverfassung vom 18. April 1999⁴⁸ (BV). Auf diese Verfassungsgrundlage stützen sich alle Bereiche, die zur Funktionsfähigkeit der Infrastruktur für das gesamte Fernmeldewesen notwendig sind. Der Gesetzgeber hat damit im FMG nicht nur das Angebot von Fernmeldediensten und die Organisation des Fernmeldemarktes geregelt, sondern auch zahlreiche Vorschriften über die Ressourcen (Frequenzen, Adressierungselemente), und die Infrastrukturen (Anlagen, Kabelkanalisationen) erlassen.

Die im Rahmen dieser Revision anvisierten Schutzmassnahmen zur Resilienz der Fernmeldeinfrastrukturen beruhen massgeblich auf dieser Verfassungsgrundlage. Die vorgeschlagenen Bestimmungen fokussieren dabei auf die technische Sicherheit der Fernmeldeinfrastruktur an sich. Darüber hinaus sollen sie aber auch zur strukturellen Unabhängigkeit der Schweiz beitragen und dadurch der Wahrung der inneren und äusseren Sicherheit dienen. Es rechtfertigt sich daher, die vorliegende Revision und insbesondere die Artikel 48a ff. auch auf Artikel 173 Absatz 2 BV zu stützen.

Der Schutz vor Cyberbedrohungen umfasst jedoch nicht nur die Fernmeldeinfrastruktur, sondern auch die darüber erbrachten Dienste und damit letztendlich auch die Bevölkerung als Benutzende dieser Dienste. Während die Verfassungsgrundlagen in Artikel 92 und 173 Absatz 2 BV den Schutz der Fernmeldeinfrastruktur und der Sicherheit und Unabhängigkeit der Schweiz vorsehen, sollen sich die Bestimmungen zum Schutz der Benutzerinnen und Benutzer zusätzlich auf Artikel 97 stützen. Diese Kompetenz erlaubt dem Bund Massnahmen zum Schutz der Konsumentinnen und Konsumenten zu erlassen und dient daher als Grundlage für den Erlass der vorgesehenen Jugend- und Konsumentenschutzbestimmungen namentlich in den Artikeln 6a, 6b sowie 46a.

Art. 1 *Zweck*

Abs. 1

Das FMG verfolgt den Zweck, dass der Bevölkerung und der Wirtschaft vielfältige, preiswerte, qualitativ hochstehende sowie national und international konkurrenzfähige Fernmeldedienste angeboten werden. Es schafft dazu die notwendigen regulatorischen Rahmenbedingungen. Mit Blick auf die zunehmende Gefährdung durch Cyberbedrohungen, kann das Ziel nur gewährleistet werden, wenn dem Aspekt der technischen Sicherheit in Bezug auf die Fernmeldeinfrastruktur und der darüber erbrachten Dienste genügend Rechnung getragen wird. Der Grundzweck des FMG soll daher mit dem Aspekt der Sicherheit in Absatz 1 ergänzt werden. So sollen die Bevölkerung und die Wirtschaft nicht nur über qualitativ hochstehende Fernmeldedienste verfügen, sondern auch sichere Dienste benutzen können. Der mittlerweile wesentliche Aspekt der Sicherheit ist dabei in einem technischen und betrieblichen Sinne zu verstehen. Wie bis anhin sollen insbesondere die Anbieterinnen dabei keine Überprüfung von Inhalten vornehmen, diese bleiben durch das Prinzip des Fernmeldegeheimnisses (vgl. Art. 43

⁴⁸ SR 101

FMG und Art. 13 Abs. 1 BV, 321^{ter} des Strafgesetzbuchs vom 21. Dezember 1937⁴⁹ [StGB]) geschützt.

Abs. 2

Der in Absatz 1 neu festgelegte Grundsatz des Angebots von sicheren Fernmelde-diensten soll in den abgeleiteten Zielen in Absatz 2 ebenfalls festgehalten und konkre-tisiert werden. Dies insbesondere auch, damit der Gesetzgeber wie auch der Bundesrat normativ tätig werden können.

Bst. b

Die explizite Nennung der Sicherheit und des Schutzes vor Cyberbedrohungen in Buchstabe b bezieht sich auf den störungsfreien Fernmeldeverkehr an sich, wobei gleichzeitig die Achtung der Persönlichkeitsrechte der Benutzerinnen und Benutzer si-cherzustellen ist. Durch einen sicheren Fernmeldeverkehr soll die Bevölkerung und die Wirtschaft und somit das Rechtsgut des privaten Interesses der Benutzerinnen und Benutzer von Fernmeldediensten geschützt werden. Der Schutz vor Cyberbedrohungen als Ziel ermöglicht und rechtfertigt die Aufnahme von neuen Aufgaben und Pflich-ten in diesem Zusammenhang. So soll der Bund hinsichtlich des Schutzes vor Cyber-bedrohungen neue Konsumentenschutzaufgaben wahrnehmen können. Er soll dabei namentlich bei missbräuchlich verwendeten Adressierungselementen Sperrungen an-ordnen können, damit präventiv kriminelle Absichten rasch und effektiv unterbunden werden können (vgl. Art. 6a und 6b) und so die Bevölkerung vor Vermögens- und Per-sönlichkeitsrechtsverletzungen geschützt wird.

Angesichts der Notwendigkeit, die Rechtsvorschriften im Bereich der Cybersicherheit zu koordinieren und zu harmonisieren, soll der Begriff der Cyberbedrohung im FMG der Definition in Artikel 5 Buchstabe f (i. V. m. Buchstabe a und d) ISG entsprechen. Es handelt sich dabei um jeden Umstand oder jedes Ereignis mit dem Potenzial, einen Cybervorfall zu ermöglichen; also einem Ereignis bei der Nutzung von Mitteln der In-formation- und Kommunikationstechnik das dazu führt, dass die Vertraulichkeit, Ver-fügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbei-tung beeinträchtigt ist.

Bst. f

Die Verankerung der Resilienz und der Sicherheit der Fernmeldeinfrastrukturen im Zweckartikel soll die Wichtigkeit der Sicherheit im Bereich der Infrastruktur an sich und darüber hinaus auch der strukturellen Unabhängigkeit und der Cyberresilienz der Schweiz unterstreichen.

Auch wenn die Verankerung der Sicherheit und der Resilienz im Endeffekt ebenfalls der Wirtschaft und der Bevölkerung zugutekommt, wird vorderhand der Schutz des Rechtsgutes des öffentlichen Interesses der inneren und äusseren Sicherheit und da-mit den Schutz des Werk-, Wirtschafts- und Finanzplatzes der Schweiz bezweckt. So zielt die Resilienz der Fernmeldeinfrastruktur denn auch auf die Gewährleistung der strukturellen Unabhängigkeit der Schweiz mit Blick auf die geopolitische Lage ab. Die

⁴⁹ SR 311.0

Festlegung im Zweckartikel dieser Grundsätze rechtfertigt und ermöglicht es dem Gesetzgeber wie dem Bundesrat auch in diesem Bereich normativ tätig zu werden und sowohl Pflichten für die Marktakteure wie auch Aufgaben für den Bund vorzusehen.

Demnach sollen Anbieterinnen von Fernmeldediensten technische, operative und administrative Massnahmen ergreifen, um die unbefugte Manipulation von Fernmeldeinfrastrukturen durch fernmeldetechnische Übertragungen und andere Cyberbedrohungen zu bekämpfen, womit die Resilienz der Fernmeldeinfrastrukturen verbessert wird (vgl. Art. 48a). Dabei haben die Anbieterinnen sowohl bei der Konzeption wie auch beim Betrieb ihrer Fernmeldeinfrastrukturen sichere Bestandteile zu verwenden und eine Diversifizierungsstrategie zu verfolgen (vgl. Art. 48b). Im Sinne einer *ultima ratio* soll es zudem dem Bundesrat möglich sein, Massnahmen im Falle einer Zuspitzung der geopolitischen Lage ergreifen zu können (vgl. Art. 48c).

Art. 3 Begriffe

Bst. d Fernmeldeanlagen

Die Ergänzung der Definition von Fernmeldeanlagen in Artikel 3 Buchstabe d mit dem Begriff Software trägt den stetigen technologischen Fortschritten und der inzwischen allgegenwärtigen Integration von Software in den Fernmeldeanlagen Rechnung. Software kann nicht vernachlässigbare Auswirkungen auf die Konformität von Fernmeldeanlagen haben, da sie eine vollständige Kontrolle der Anlage ermöglicht, in die sie integriert ist. Sie bietet dem Hersteller die Flexibilität zur Erweiterung der Funktionen seines Produkts oder zur Fehlerbehebung durch ein einfaches Update, das den Benutzerinnen und Benutzern zur Verfügung gestellt werden kann. Gemeint ist hier ausschliesslich Software, die sich auf die Konformität mit den grundlegenden Anforderungen auswirken könnte. Die FAV enthält bereits verschiedene Bestimmungen betreffend Software in Funkanlagen. Mit der Aufnahme des Begriffs Software in die Definition von Fernmeldeanlagen wird nun auch für diese klargestellt, dass Software als Teil von ihnen gilt.

Art. 3a Rechte und Pflichten von Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen

Abs. 1

Mit dem neuen Artikel 3a wird eine Lücke im FMG geschlossen, welche durch neue Geschäftsmodelle und die Verwendung des Begriffs Anbieterinnen von Fernmeldediensten entstanden ist. Der Artikel trägt dem Umstand Rechnung, dass der Ausbau von Fernmeldenetzen (insbesondere von Anschlussnetzen) auch durch Unternehmen erfolgen kann, die selbst keine Fernmeldedienste anbieten, sondern lediglich Infrastruktur für die fernmeldetechnische Übertragung von Informationen für Dritte vermieten («reine Fernmeldeinfrastrukturanbieterinnen»). Vor diesem Hintergrund erscheint es logisch, dass es bei der Erstellung von Fernmeldeanschlüssen keine Rolle spielen sollte, ob das erschliessende Unternehmen dann auch Fernmeldedienste erbringt oder ob diese von einem anderen Unternehmen bereitgestellt werden. Die Bestimmung stellt klar, dass für Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten (vgl. Bst. a) oder Eigentümerinnen von Kabelkanalisationen (vgl. Bst. b) nach diesem Gesetz im Zusammenhang mit derartigen Fernmeldeinfrastrukturen die gleichen Rechte und Pflichten gelten wie für Unternehmen, welche die gleichen Infrastrukturen betreiben, aber zusätzlich Fernmeldedienste anbieten. Eine Ungleichbehandlung dieser beiden Unternehmenstypen war nie Absicht der

Fernmeldegesetzgebung. Die Klarstellung hat sich durch das vermehrte Vorhandensein des Geschäftsmodells «Betrieb von *Darkfiber*-Netzen» aufgedrängt.

Beispielhaft aufgezeigt werden kann die Lücke respektive der Klärungsbedarf an den Artikeln 35, 35a, 35b, 36, 36a und 37 im Kapitel 5 (Fernmeldeanlagen). Diese Vorschriften sind an Unternehmen adressiert, die mit eigener Netzinfrastruktur Leitungen zu Liegenschaften verlegen. Die enthaltenen Rechte und Pflichten betreffen den physischen Netzbau und es gibt keine Gründe, weshalb diesbezüglich Unternehmen, die Netze bauen aber keine Fernmeldedienste anbieten, anders behandelt werden sollten als solche, die zusätzlich selbst Fernmeldedienste anbieten. Entsprechend werden die betroffenen Artikel in Absatz 1 konkret aufgeführt.

Beim Begriff Fernmeldeanlagen in Buchstabe a kommt der Präzisierung «zur Bereitstellung von Fernmeldediensten» eine bedeutende Rolle zu: Sie sorgt dafür, dass sich der Kreis der betroffenen Personen auf Unternehmen im Fernmeldemarkt beschränkt. Eigentümer und Eigentümerinnen von beispielsweise Mobilfunkgeräten, welche diese Dritten zum Gebrauch überlassen, sind damit vom Kreis der betroffenen Personen ausgeschlossen (bspw. Eltern, die ihrem Kind ein Mobiltelefon zum Gebrauch überlassen). Demgegenüber ist eine unbeleuchtete Glasfaser, die einer Anbieterin von Fernmeldediensten zum Gebrauch überlassen wird, eine Fernmeldeanlage zur Bereitstellung von Fernmeldediensten und deren Eigentümerin hat die gleichen Rechte und Pflichten bezüglich dieser Glasfaser wie dies auch Anbieterinnen von Fernmeldediensten bezüglich Glasfasern in ihrem Eigentum haben.

Sowohl bei Buchstabe a wie auch bei Buchstabe b ist jeweils entscheidend, dass die Fernmeldeanlagen oder Kabelkanalisationen Dritten zum Gebrauch überlassen werden, um damit Fernmeldedienste zu erbringen.

Abs. 2

Sollte sich zeigen, dass für den wirksamen Wettbewerb beim Erbringen von Fernmeldediensten andere Rechte und Pflichten von Anbieterinnen von Fernmeldediensten sinngemäss für Eigentümerinnen oder und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten oder von Kabelkanalisationen gelten müssen, so kann der Bundesrat dies auf Verordnungsstufe vorsehen.

Art. 4 Registrierung

Abs. 1 und 2

Bei der letzten Revision des FMG wurde die allgemeine Meldepflicht abgelöst durch die Registrierung ausschliesslich jener Anbieterinnen von Fernmeldediensten, die für die Erbringung von Fernmeldediensten Funkfrequenzen, deren Nutzung eine Konzession voraussetzt, oder auf nationaler Ebene verwaltete Adressierungselemente nutzen. Diese Möglichkeit soll beibehalten werden und ist weiterhin in den Absätzen 1 und 2 der Bestimmung abgebildet. Der gewählte Ansatz hat sich aber in der Praxis als ungenügend erwiesen, da er den Vollzugsbehörden keine Übersicht über die Teilnehmer des Fernmeldemarktes erlaubt. Eine solche Übersicht ist aus Gründen der Transparenz (vgl. Art. 12a) und Aufsicht (vgl. Art. 58), zur Erstellung des Evaluationsberichts (vgl. Art. 3a) und der amtlichen Fernmeldestatistik (vgl. Art. 59 Abs. 2) oder als Grundlage für die Evaluation des Fernmelderechts (vgl. Art. 59 Abs. 2^{bis} Bst. c) unverzichtbar. Im Übrigen haben sich insbesondere beim Infrastrukturausbau im Zusammenhang mit

dem Entwurf des Bundesgesetzes über die Förderung des Ausbaus von Breitbandinfrastrukturen, BBFG⁵⁰ neue Bedürfnisse betreffend Marktkenntnis gezeigt. Vor diesem Hintergrund drängt sich eine Anpassung der Bestimmungen über die Registrierung auf. Aufgrund der erweiterten Registrierungsmöglichkeit des BAKOM soll die Bestimmung neu nummeriert werden, wobei die bisherigen Absätze 1 und 2 keine Änderungen erfahren.

Abs. 3

Der materielle Gehalt des bisherigen Absatz 3 soll aufgrund der neuen Struktur in Absatz 4 überführt werden. Künftig soll das BAKOM gestützt auf Absatz 3 bei Bedarf dem FMG unterliegende Personen, die keine vom BAKOM verwaltete Ressourcen nutzen, registrieren können, um insbesondere den Vollzug und die Aufsicht über die Gesetzgebung, die Erstellung der Statistik oder die Gesetzesevaluation zu ermöglichen. Die betroffenen Personen sind nach Artikel 59 Absatz 1 verpflichtet, die für die Registrierung notwendigen Auskünfte zu erteilen. Das BAKOM soll dabei insbesondere Anbieterinnen von Internetzugängen oder auch beispielsweise massgebliche Anbieterinnen von Radio- und Fernsehprogrammen erfassen können, sofern diese für den Vollzug und die Evaluation des Fernmelderechts bedeutsam sind. Des Weiteren sollen auch Eigentümerinnen respektive Betreiberinnen von Glasfaserleitungen (sog. *Darkfiber*-Anbieterinnen) und Betreiberinnen oder Eigentümerinnen von Fernmeldeanlagen, die ihre Infrastruktur anderen Anbieterinnen zum Gebrauch überlassen und keine Gebäude erschliessen, vom BAKOM registriert werden können.

Mit dieser neuen Registrierungsmöglichkeit entstehen für die betroffenen Akteure keine neuen materiellen Rechte und Pflichten. Diese unterliegen bereits heute dem Fernmelderecht. Vielmehr dient die erweiterte Registrierungsmöglichkeit dem BAKOM, die massgeblichen Marktteilnehmer vollständig abbilden zu können und dank einer umfassenden Datengrundlage seine Aufgaben zweckmässig erfüllen zu können.

Reine Eigentümerinnen oder Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen, die damit Gebäude fernmeldetechnisch erschliessen, sind von diesem Absatz nicht betroffen. Für sie gilt die Meldepflicht nach Artikel 4a.

Abs. 4

Die Angaben über die registrierten Anbieterinnen, Betreiberinnen oder Eigentümerinnen sollen im Rahmen einer Liste erfasst werden können. Dabei sollen insbesondere auch die angebotenen Dienste wie auch die Fernmeldeanlagen registriert werden können. Mit der Präzisierung, dass das BAKOM die Liste der registrierten Personen veröffentlichen kann, wird die Pflicht zur Veröffentlichung dieser Liste aufgehoben. Das BAKOM soll sich jedoch wie bisher aus Transparenzgründen weiterhin bemühen, diese Liste zu veröffentlichen, respektive es sollte nur bei gänzlich fehlendem Interesse an einer Veröffentlichung darauf verzichten.

Abs. 5

Der Bundesrat soll Ausnahmen von der Registrierung vorsehen können. Denkbar sind insbesondere Konstellationen, in welchen eine Anbieterin für eine kurze Zeit Adressierungselemente oder konzessionierte Frequenzen zur Erbringung eines Fernmeldedienstes beantragt und die Dienste dabei nur im Rahmen von Artikel 2 FDV erbringt.

⁵⁰ Siehe abgeschlossene Vernehmlassungen 2025: https://fedlex.data.admin.ch/eli/dl/proj/2025/4/cons_1.

Solche in sich geschlossene Dienstleistungen sollen vom BAKOM grundsätzlich nicht registriert werden müssen. Namentlich nicht, wenn sich die mit der Dienstleistung erforderlichen Ressourcen auf eine kurze Zeit (z.B. während der Dauer eines Musikfestivals) begrenzen.

Art. 4a Meldepflicht

Abs. 1

Um den derzeitigen Stand des Ausbaus der Fernmeldeinfrastruktur genau und vollständig zu beschreiben, muss definiert werden, welche Informationen erhoben werden sollen. Im konkreten Fall handelt es sich um die Fernmeldeanlagen, mit welchen Gebäude fernmeldetechnisch erschlossen werden und tatsächlich oder theoretisch für die Erbringung eines Fernmeldedienstes nach Artikel 3 Buchstabe b nutzbar sind.

Zur Erlangung dieser Informationen ist festzulegen, wer sie zur Verfügung zu stellen hat, und vor allem sicherzustellen, dass das BAKOM mit den betroffenen Personen in Verbindung treten kann. Um Verwirrung zu vermeiden und sämtliche Infrastrukturen – auch die inaktiven – zu erfassen, sind sowohl die Eigentümerinnen wie auch die Betreiberinnen entsprechender Fernmeldeanlagen der Meldepflicht zu unterstellen.

Damit die mit Artikel 4 anvisierte Gesamtübersicht der auf dem Schweizer Fernmeldemarkt aktiven Akteure erstellt werden kann, sollen auch meldepflichtige Unternehmen nach Artikel 4a vom BAKOM registriert werden können.

Abs. 2

Es ist Aufgabe des Bundesrates, die Form und den Inhalt der Meldepflicht und der Registrierung dieser Akteure auszugestalten sowie Vorgaben festzulegen, damit die Liste der Eigentümerinnen oder Betreiberinnen vollständige und aktuelle Angaben enthält.

Art. 6a Sperrung des Zugangs zu Fernmeldediensten

Abs. 1

Anbieterinnen von Fernmeldediensten in der Schweiz sind verpflichtet, ihre Kundinnen und Kunden gemäss den überwachungsrechtlichen Vorgaben zu identifizieren. Die Beschränkung der geltenden Sperrpflicht der Anbieterinnen von Fernmeldediensten auf Angebote ohne Abonnementsverhältnis hat sich in der Praxis als zu wenig weitreichend erwiesen. Die Problematik, dass eine Identifikation der Kundinnen und Kunden bei der Aufnahme der Kundenbeziehung nachträglich als falsch oder nicht entsprechend den überwachungsrechtlichen Vorgaben dokumentiert herausstellte, trat ursprünglich vor allem bei mobilen Angeboten – Sprachtelefonie oder Internetzugang – mit vorausbezahltem Guthaben (*prepaid*) auf. Zu falschen oder nicht bestimmungsgemässen Identifikationen kam es oft aufgrund von Nachlässigkeiten oder durch täuschendes Verhalten der Benutzenden. Das war denn auch der Grund für die Einführung dieser Bestimmung mit einem auf diese Fälle beschränkten Anwendungsbereich.

Seit Inkrafttreten der Bestimmung hat sich gezeigt, dass dieselben Probleme vor allem für die Strafverfolgungsbehörden auch in Zusammenhang mit anderen Angeboten, so zum Beispiel Festnetzangeboten mit Rechnungsstellung (*postpaid*), in Erscheinung treten.

Personen, die sich nicht identifizieren lassen wollen, um sich einer möglichen strafrechtlichen Verfolgung entziehen zu können, nutzen bei den *postpaid* Angeboten ebenfalls gefälschte Dokumente, die sie zwecks einer vermeintlichen Identifikation verwenden. Die Dokumente lassen sich mit digitalen Werkzeugen zunehmend einfacher, schneller und in einer täuschend echten Qualität erstellen, wobei insbesondere die Verwendung von künstlicher Intelligenz neue und ungeahnte Möglichkeiten bietet. Zudem werden auch illegal erlangte Zahlungsmittel oder solche, die eine Rückverfolgung erschweren oder gänzlich verunmöglichen, genutzt.

Aus den dargelegten Gründen wird mit der vorliegenden Anpassung der Anwendungsbereich auf alle Vertragsverhältnisse ausgedehnt und findet nun unabhängig davon Anwendung, wie die Rechnungsstellung erfolgt oder welche Nummernkategorie (Festnetz- oder Mobilnummer) involviert ist. Durch die Ausdehnung auf zusätzliche Anwendungsfälle werden jedoch keine neuen Rechte oder Pflichten für die Anbieterinnen von Fernmeldediensten geschaffen.

Bst. a

Buchstabe a sieht eine Sperrung vor, wenn bei der Identifikation durch die Anbieterin eine fiktive Identität (vgl. Ziff. 1) oder die Identität einer unbeteiligten Person ohne deren Einwilligung verwendet wurde (vgl. Ziff. 2). Buchstabe a entspricht der geltenden Regelung, die in diesen beiden Fällen ebenfalls schon eine Sperrung von (*postpaid*) Angeboten vorsieht. Buchstabe a wird aufgrund der Ausdehnung des Anwendungsbereichs neu formuliert und neu strukturiert.

Bst. b

Insbesondere Anbieterinnen mit Sitz im Ausland, die ihren Kundinnen und Kunden im Ausland einen Zugang zu Telefonie und Internet zur Verfügung stellen, sind unter Umständen überhaupt nicht verpflichtet eine Identifikation vorzunehmen - weder gemäss inländischen Vorschriften noch gemäss den Vorgaben des Bundesgesetzes vom 18. März 2016⁵¹ betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Aus Sicht der Anbieterin mit Sitz im Ausland handelt es sich bei den Vorschriften des BÜPF um ausländische Vorgaben. Bestehen im Land, in dem die Anbieterin ihren Sitz hat, gar keine entsprechenden Vorgaben oder nur solche, die nicht mit denjenigen in der Schweiz vergleichbar sind, müssen die Anbieterinnen den Zugang ebenfalls sperren. Kommen sie den Sperrungen nicht nach, droht ihnen im Rahmen von aufsichtsrechtlichen Verfahren der Verlust des Rechts, schweizerische Nummern für Fernmeldedienste ihren Kundinnen und Kunden zur Verfügung stellen zu können. Daneben droht eine verwaltungsrechtliche Sanktion. Als gleichwertig werden Vorgaben betrachtet, welche eine vergleichbare Identifikation der Benutzenden wie in der Schweiz anhand von amtlichen Dokumenten vorsehen. Buchstabe b entspricht, wie Buchstabe a, der geltenden Regelung, die unverändert in die neu strukturierte Bestimmung übernommen wird.

Bst. c

Buchstabe c trägt dem Umstand Rechnung, dass Informationen betreffend die Identifikation der Benutzenden aus technischen oder rechtlichen Gründen oftmals nicht innert nützlicher Frist aus dem Ausland an die Schweizer Behörden übertragen werden kön-

⁵¹ SR 780.1

nen respektive dürfen, selbst wenn eine dem Schweizer Recht als gleichwertig entsprechende Pflicht dazu im betreffenden Land besteht, in dem der Zugang zur Verfügung gestellt wird. Im Gegensatz zu Buchstabe b entspricht die Identifikation im Land, in dem der Zugang zur Verfügung gestellt wird, dem Umfang und der Qualität den überwachungsrechtlichen Vorgaben in der Schweiz. Aufgrund von datenschutzrechtlichen Vorgaben dürfen Personendaten oftmals nicht grenzüberschreitend übertragen werden. Vielmehr müssen dazu die vorgesehenen Wege über die internationalen Rechtshilfeverfahren bestritten werden. Diese Verfahren sind in der Regel von langer Dauer. In diesem Fall sperren die Anbieterinnen von Fernmeldediensten somit den Zugang bis zur Übertragung der Angaben nach dem dafür vorgesehenen internationalen Rechtshilfeverfahren. Anhand der übertragenen Informationen kann in der Folge geprüft werden, ob die Sperrvoraussetzungen gegebenenfalls nach Buchstaben a und b gegeben sind. Sollte dies der Fall sein, ist die Sperrung aufrecht zu erhalten; sind keine der beiden Voraussetzungen gegeben, ist die Sperrung aufzuheben.

Abs. 2

Bei einer Sperrung nach Absatz 1 haben die zuständigen Strafverfolgungsbehörden sicherzustellen, dass keine Sperrung erfolgt, wenn die Telefonnummer oder der Internetzugang Gegenstand eines Überwachungsauftrags des Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ist. Die zuständigen Behörden müssen dies sicherstellen, soweit ihnen der Umstand einer laufenden Überwachung bekannt ist. In diesen Fällen erfolgt eine Rücksprache mit dem Dienst ÜPF.

Art. 6b Widerruf und Sperrung von Telefonnummern und Domain-Namen

Abs. 1

Telefonnummern werden oft für betrügerische Aktivitäten missbraucht. Die Täterschaft setzt die geografischen Nummern, oftmals aus dem Vorwahlbereich des Wohnortes der (potenziellen) Opfer, als vertrauenerweckende Kontaktmöglichkeit ein und täuscht dabei einen vermeintlich in der Schweiz liegenden Ursprung vor. Die Täter bringen die Opfer über diese Kontakte und unter Vorspiegelung weiterer falscher Tatsachen (z. B. angeblicher Angestellter der regionalen Filiale der Bank des Opfers) oftmals zu vermögensschädigenden Handlungen mit hohen Schadenssummen. Um dieses Phänomen proaktiv zu bekämpfen, soll mit dem neuen Artikel 6b eine neue, rasche und effiziente Sperrmöglichkeit eingeführt werden.

Die vorgeschlagene fünftägige Sperrung bei einem begründeten Verdacht auf einen mutmasslichen Betrug gemäss Artikel 146 StGB stellt dabei einen präventiven Akt dar, damit nicht weitere Personen Opfer eines solchen Betrugsmodells werden. Es geht darum, die Täterschaft in ihrem Vorgehen zu stören und die laufenden Aktionen zu unterbrechen (sog. *Crime Disruption*). Es handelt sich nicht um eine strafrechtliche Verfolgung solcher Betrugsformen, sondern um eine Schutzmassnahme für die Nutzenden der Fernmeldedienste, welche gleichzeitig auch die missbräuchliche Verwendung von Adressierungselementen unterbinden soll. Die mit Hilfe von Telefonnummern vorgenommenen betrügerischen Tätigkeiten verursachten Schäden ereignen sich schnell und zahlreich, wenn nicht innert kurzer Frist der Zugang zu der benutzten Telefonnummer gesperrt werden kann. Die Vorgehen lassen sich denn auch ohne grösseren Aufwand adaptieren oder kopieren, wenn die Täterschaft feststellt, dass eine laufende Aktion keine Beute mehr einbringt. Ein entstandener Schaden, insbesondere ein Vermögens- oder auch Datenverlust, ist in der Regel irreparabel und die international operierende Täterschaft kann kaum belangt werden. Eine schnelle Sperrung ist daher der

entscheidende Faktor, um die Konsumentinnen und Konsumenten vor solchen Gefahren zu schützen. Damit eine Nummer gesperrt werden kann, muss wie in Absatz 2 ein begründeter Verdacht vorliegen (vgl. nachfolgende Ausführungen). Die Sperrung erfolgt dabei durch die Anbieterinnen von Fernmeldediensten auf Hinweis von fedpol.

Abs. 2

Da im Rahmen solcher Cyber-Betrugsformen nicht nur Telefonnummern, sondern auch Domain-Namen verwendet werden, soll diese Sperranweisung auch für Schweizer Domain-Namen Geltung haben, sofern diesbezüglich die Voraussetzungen nach Absatz 1 erfüllt sind. Entsprechend werden hierzu auch die zuständigen Registerbetreiberinnen in die Pflicht genommen.

Mit dem vorgesehenen Mechanismus nach den Absätzen 1 und 2 wird dem Bedürfnis nach schnellem, effizientem und zielgerichtetem Agieren im Kampf gegen Cyberbedrohungen Rechnung getragen. Damit wird auch den Anliegen der Motion Götte (24.4393) nachgekommen. Diese verlangt, dass nicht mehr nur *Phishing* oder *Malware* als Voraussetzungen für die technische und administrative Blockierung der Domain gemäss Artikel 15 ff. VID gelten, sondern auch weitere strafrechtlich relevante Handlungen (z. B. alle Vergehens- und Verbrechenstatbestände, sowie Versuche dazu) abgedeckt werden. Dieser Forderung in der VID nachzukommen und auf sämtliche Vergehens- und Verbrechenstatbestände auszudehnen, wäre mit Blick auf das Legalitätsprinzip problematisch.

Die in Artikel 15 ff. VID vorgesehenen Sofortmassnahmen zur Sperrung von Domain-Namen gelten nur im Zusammenhang mit Cyberkriminalität, die unter *Phishing* oder die Verbreitung und Nutzung von *Malware* (*Botnets* oder Botnetze) fällt. Jegliches andere illegale Verhalten als Grundlage für die Sperrung ist ausgeschlossen. Es ist daher nicht möglich, Domain-Namen mit der Endung *.ch* oder *.swiss* zu sperren, wenn sie für Straftaten wie Betrug benutzt werden. Der Anwendungsbereich von Artikel 15 ff. VID beschränkt sich mithin auf technisch offensichtliche Angriffe wie die Verbreitung von *Malware* oder *Phishing*. Dabei handelt es sich um Angriffe, die in der Regel automatisiert sind, methodisch auf das *Domain Name System* (DNS) zurückgreifen und daher objektiv und ohne materielle Wertung identifiziert werden können. Nur bei solchen technischen Angriffen kann die Registerbetreiberin von *.ch* oder *.swiss* nach Artikel 15 Absatz 1 VID berechtigt sein, Massnahmen zu ergreifen, die sich auf die Nutzung eines Domain-Namens beziehen. Dieser restriktive Ansatz entspricht dem Ansatz der globalen DNS-Verwaltungsorganisation (*Internet Corporation for Assigned Names and Numbers*, ICANN), die der Ansicht ist, dass sich die Missbrauchsbekämpfung durch die DNS-Akteure ausschliesslich auf Fälle von *Malware*, *Botnets*, *Phishing* (mit dem damit verbundenen *DNS-Pharming*) und Spam, wenn es als Vektor für die Verbreitung von Malware oder Phishing dient, beschränken soll.

Die Ausweitung des Geltungsbereichs von Artikel 15 VID auf weitere strafrechtlich relevante Handlungen ist hinsichtlich der Achtung der Grundrechte und der Garantien des Rechtsstaats problematisch. Eine solche Ausweitung des Interventionsbereichs der Akteure des DNS kann nicht in einer Verordnung des Bundesrates wie der VID ihren Platz finden, welche zudem technisch und administrativ geprägt ist. Vielmehr muss eine Ausdehnung der Interventionsmöglichkeiten auf Ebene eines formellen Gesetzes geregelt werden. Damit fedpol im Bereich von Cyberbedrohungen präventiv tätig werden kann, wird mit Artikel 6b eine Regelung auf Gesetzesstufe geschaffen.

Für eine Sperrung nach dieser Bestimmung soll der begründete Verdacht auf einen mutmasslichen Betrug ausreichend sein. Ein begründeter Verdacht bedeutet, dass ein Sachverhalt gegeben ist, bei dem eine Rechtsverletzung vermutet wird und hinreichende Anhaltspunkte vorliegen, die deren Wahrscheinlichkeit belegen. Er unterscheidet sich von einer vagen Vermutung durch das Erfordernis einer gewissen Wahrscheinlichkeit, dass die Tat tatsächlich begangen wurde. Diese Wahrscheinlichkeit wiederum basiert auf Fakten und Anzeichen, die aufgrund der Erfahrung für die Annahme einer Straftat sprechen. Der begründete Verdacht ist eine Zwischenstufe zwischen vager Vermutung und vollem Beweis. Wenn das BACS konkrete Meldungen seitens der Polizei oder der Bevölkerung erhält, mehrere ähnlich gelagerte Fälle vorliegen oder wenn sich aufgrund der Erfahrungswerte des BACS ein Verdacht eines möglichen Betrugs aufdrängt, kann ein begründeter Verdacht als gegeben betrachtet werden. In solchen Fällen soll das BACS die erhaltenen Informationen aus Meldungen nach Artikel 73b ISG an fedpol mitteilen und fedpol bei der Beurteilung unterstützen, damit dieses den Hinweis zur Sperrung an die betroffenen Anbieterinnen oder Registerbetreiberinnen vornehmen kann (vgl. Abs. 3). Dabei handelt es sich nicht um eine strafrechtliche Verfolgung seitens fedpol, sondern um ein präventives Einschreiten, so dass der Betrug an sich verhindern werden kann. Die mutmasslichen Online-Betrugsformen werden in den allermeisten Fällen von bandenmässig organisierten Täterschaften begangen. Als zuständige Strafverfolgungsbehörde im Bereich der organisierten Kriminalität kennt fedpol die Vorgehensweisen entsprechender Täterschaften gut und ist daher in der Lage, rasch entsprechende Verhaltensweisen zu analysieren und zu erkennen. Seine Zuständigkeit legitimiert sich aber auch durch die Tatsache, dass grundsätzlich die gesamte Bevölkerung unabhängig des Wohnortes vor solchen Betrugsformen geschützt werden soll. Im Gegensatz dazu ist der vollzogene Betrug klarerweise von den zuständigen kantonalen Strafverfolgungsbehörden zu verfolgen. Gestützt auf Artikel 23 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007⁵² (Strafprozessordnung, StPO) ist die Bundesgerichtsbarkeit für Betrugsdelikte dabei ausgeschlossen, woran sich auch aufgrund dieser neuen Aufgabe von fedpol nichts ändern soll.

Abs. 3

Das BACS erhält Meldungen über Cyberbedrohungen gemäss Artikel 73b ISG und geht diesen nach. Das BACS soll diese Meldungen sodann fedpol zur Verfügung stellen und fedpol bei der Beurteilung dieser Fälle unterstützen. Bei einem begründeten Verdacht auf einen mutmasslichen Betrug soll fedpol schnell eine Sperre bei der betreffenden Fernmeldediensteanbieterin oder Registerbetreiberin verlangen können.

Abs. 4

Da die Sperrung lediglich aufgrund eines begründeten Verdachts erfolgt, darf sie höchstens fünf Tage dauern. Danach muss eine Staatsanwaltschaft oder ein Gericht eingeschaltet werden, welches im Rahmen seiner Zuständigkeit als Strafverfolgungsbehörde eine längere Sperre bei der in Frage stehenden Fernmeldediensteanbieterin (für Telefonnummern) oder Registerbetreiberin (für Domain-Namen) anordnen kann. Dies ist aus Gründen der Rechtsstaatlichkeit und der Gewaltentrennung geboten. Zudem kann die Staatsanwaltschaft oder das Gericht bis zum Abschluss eines allfälligen Strafverfahrens die betroffenen Telefonnummern oder Domain-Namen sperren lassen.

⁵² SR 312.0

Abs. 5

Bei der Sperrung von Telefonnummern ist weiter durch die zuständigen Behörden sicherzustellen, dass keine Sperrung erfolgt, wenn die betroffene Nummer Gegenstand eines Überwachungsauftrags des Dienstes ÜPF ist. Sie stellen dies sicher, soweit ihnen der Umstand einer laufenden Überwachung bekannt ist. In diesen Fällen erfolgt eine Rücksprache mit dem Dienst ÜPF.

Art. 13 Auskunft durch das BAKOM

Abs. 1

Bst. a

Mit der Gesetzesrevision sollen zum einen eine erweiterte Registrierungsmöglichkeit (vgl. Art. 4) und zum andern eine Meldepflicht für bestimmte Marktakteure (vgl. Art. 4a) eingeführt werden. Die neuen Vorgaben erstrecken sich insbesondere auf die in Artikel 4 Absatz 3 sowie Artikel 4a genannten Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen. Artikel 13 trägt dieser Weiterentwicklung Rechnung und ergänzt die bereits bestehende Bestimmung mit den zusätzlichen Akteuren. Dabei ändert sich nichts am Grundsatz, dass die Auskunft nur erteilt werden kann, sofern keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen. Nicht unter das Auskunftsrecht fallen jedoch Auskünfte zu Anbieterinnen und deren Fernmeldeanlagen und Vorrichtungen nach den Artikel 32a (Störsender) und 32b (Sonderelektronik). Diesbezüglich bestehen öffentliche Interessen zum Schutze der Sicherheit, die gegen eine Auskunft über diese Anlagen sprechen. Aus materieller Sicht bleibt die Auskunft nach Buchstabe a wie im geltenden Recht auf den Namen und die Adresse beschränkt.

Bst. b

Da das BAKOM künftig auch weitere Marktakteure registrieren können soll, soll es auf Anfrage auch Auskünfte über die von ihnen erbrachten und bereitgestellten Dienste erteilen können, sofern hierzu wiederum keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen. Unter die Auskunft zum Dienstangebot können auch die durch eine Akteurin angebotenen oder betriebenen Fernmeldeanlagen oder die angebotene Technologie (z.B. Glasfaser, Satellitenangebote, etc.) fallen.

Bst. c

Die unter Buchstabe c genannten Verwaltungssanktionen beziehen sich insbesondere auf Massnahmen, die gestützt auf die Artikel 58 und 60 FMG verhängt werden. Der Wortlaut der Bestimmung wird an die Legaldefinition von Artikel 5 Buchstabe c Ziffer 5 des Bundesgesetzes vom 25. September 2020⁵³ über den Datenschutz (DSG) angepasst, auf den sich die Bestimmung bezieht.

Durch diese Änderungen in den Buchstaben a-c sollen aber keine weitergehenden Informationen und Daten im Rahmen von Auskünften erteilt werden können, als dies unter dem geltenden Recht möglich ist.

⁵³ SR 235.1

Abs. 3

Absatz 3 der geltenden Bestimmung wird aufgehoben, da sie bisher noch nie angewendet wurde (kein konkreter Bedarf) und im Übrigen heikle Fragen hinsichtlich der Verfahrensgarantien und der Rechte der Parteien aufwirft.

Art. 13a Datenbearbeitung

Die geltende Fernmeldegesetzgebung ist insbesondere in terminologischer Hinsicht nicht mehr übereinstimmend mit dem revidierten DSG, wenn es um eine angemessene Regelung der Bearbeitung von Personendaten geht. Der Geltungsbereich des DSG erstreckt sich im Übrigen nicht mehr auf die Daten juristischer Personen. Deren Bearbeitung ist heute im Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997⁵⁴ (RVOG) geregelt. Folglich sind die Artikel 13a und 13b an die Vorgaben des DSG anzupassen und es ist ein neuer Artikel 13c über die Bearbeitung von Daten juristischer Personen einzuführen.

Abs. 1

Die Fernmeldegesetzgebung enthält keinen abschliessenden Katalog der von den zuständigen Behörden zu bearbeitenden Personendaten. Welche Daten verarbeitet werden dürfen, bestimmt sich nach den jeweiligen gesetzlichen Aufgaben der ComCom, des BAKOM und der Beauftragten anhand der Fernmeldegesetzgebung. Gemäss Datenschutzrecht genügt die gesetzliche Grundlage dann, wenn die Datenbearbeitung sich direkt aus der gesetzlichen Aufgabe ergibt, dazu erforderlich ist und das Risiko einer Grundrechtsverletzung gering ist⁵⁵.

Neben der ComCom und dem BAKOM sollen neu auch die im Fernmelderecht bezeichneten Beauftragten ausdrücklich genannt werden, um ihnen eine gesetzliche Grundlage für die Bearbeitung von Personendaten einzuräumen. Als Bundesorgan im Sinne von Artikel 5 Buchstabe i DSG gelten Behörden oder Dienststellen des Bundes oder Personen, die mit öffentlichen Aufgaben des Bundes betraut sind. Mit der vorgeschlagenen Ergänzung von Artikel 13a FMG wird eine explizite Rechtsgrundlage geschaffen, welche die Delegation und die Datenbearbeitung durch die im Fernmelderecht genannten Beauftragten rechtlich klar absichert. Die Stiftung SWITCH beispielsweise ist mit der Verwaltung des Registers der .ch-Domain-Namen beauftragt (vgl. Art. 28a). Die in Artikel 12c erwähnte Schlichtungsstelle interveniert bei Streitigkeiten zwischen Kundinnen oder Kunden und Anbieterinnen von Fernmelde- oder Mehrwertdiensten (vgl. Art. 12c FMG i. V. m. Art. 42 ff. FDV). Um eine ordnungsgemässe Ausführung dieser öffentlichen Aufgabe betreffenden Aufträge sicherzustellen, müssen die Beauftragten zur Bearbeitung von Personendaten gesetzlich ermächtigt sein (vgl. Art. 34 Abs. 1 und 5 Bst. i DSG).

Es dürfen explizit nur diejenigen Personendaten bearbeitet werden, die für die Erfüllung der jeweiligen fernmelderechtlichen Aufgabe unbedingt erforderlich sind; jede darüber hinausgehende Verarbeitung ist untersagt.

Im Übrigen könnten bestimmte Entscheidungen des BAKOM in Form einer automatisierten Einzelentscheidung nach Artikel 21 Absatz 4 DSG ergehen. Wie im DSG vor-

⁵⁴ SR 172.010

⁵⁵ Bundesamt für Justiz (2024), Kap. 3.1.1, S. 15.

gesehen, kennzeichnet das BAKOM diese Entscheidungen als solche, damit die betroffenen Personen erkennen, dass sie nicht von einer natürlichen Person stammen (Transparenzprinzip). Da diese Situation durch das DSG abgedeckt ist und die Entscheidungen des BAKOM grundsätzlich nicht zu einem schwerwiegenden Eingriff in die datenschutzrechtlichen Grundrechte der betroffenen Person führen können, muss sie im FMG nicht spezifisch und formell geregelt werden.

Art. 13b Amts- und Rechtshilfe

Artikel 13b präzisiert unter welchen Voraussetzungen die zuständige Behörde – die ComCom, das BAKOM oder die mit Aufgaben Beauftragten – im Rahmen der Amtshilfe anderen Behörden in der Schweiz und im Ausland Daten übermitteln darf (vgl. Abs. 1–3). Als Schweizer Behörden kommen namentlich die Nationale Alarmzentrale (vgl. Art. 96 Abs. 2 FDV), das Bundesamt für Statistik (vgl. Art. 97 Abs. 3 FDV; Art. 51 Bst. c VID), das Eidgenössische Institut für Geistiges Eigentum und die kantonalen Handelsregister (vgl. Art. 51 Bst. c VID) in Betracht. Es ist dabei nicht ausgeschlossen, dass auch eine Datenbekanntgabe mit anderen Behörden erfolgen muss. Diese Bestimmung gilt auch für eine Übermittlung der Daten zwischen dem ComCom, dem BAKOM und den Beauftragten.

Diese Regelung erlaubt lediglich die Übermittlung von Personendaten, die im Rahmen von Artikel 13a vom BAKOM, der ComCom und den Beauftragten bei der Erfüllung der ihnen durch das Fernmeldegesetzgebung übertragenen Aufgaben beschaffen wurden. Mit der Anpassung des Artikels unter Berücksichtigung der neuen Terminologie des DSG ist nun auch der Austausch von besonders schützenswerten Daten und Resultaten von in Rahmen dieses Gesetzes durchgeführten Profilings möglich (vgl. Art. 30a Abs. 4 und 48d Abs. 5 FMG). Die Einzelheiten der Bekanntgabe von personenbezogenen und besonders schützenswerten Daten im Rahmen der Amtshilfe bleiben damit klar festgelegt.

Art. 13c Bearbeitung und Bekanntgabe von Daten juristischer Personen

Handelt es sich bei den betroffenen Personen um juristische Personen, unterliegt die Bearbeitung ihrer Daten im Prinzip nicht mehr dem DSG (vgl. Art. 2 Abs. 1 DSG), da dieses ausschliesslich Daten von natürlichen Personen schützt. Der am 1. September 2023 in Kraft getretene Artikel 57r Absatz 1 RVOG schafft eine allgemeine gesetzliche Grundlage für die Bearbeitung von Daten juristischer Personen durch Bundesorgane wie die ComCom und das BAKOM, soweit die Erfüllung ihrer in einem Gesetz im formellen Sinn umschriebenen Aufgaben dies erfordert. Vor diesem Hintergrund wird in Absatz 1 lediglich auf Artikel 13a verwiesen, der die Bearbeitung von Daten beinhaltet, die für den Vollzug und die Evaluation der Fernmeldegesetzgebung nötig sind (zu den Aufgaben im Fernmeldebereich vgl. die Ausführungen zu Art. 13a Abs. 1). Als mit einer öffentlichen Aufgabe des Bundes betraute Personen werden die Beauftragten nach diesem Gesetz den Bundesorganen gleichgestellt (vgl. Art. 5 Bst. i DSG sinngemäss).

Für die Bekanntgabe von Daten juristischer Personen müssen die Bundesorgane über eine gesetzliche Grundlage verfügen (vgl. Art. 57s Abs. 1 RVOG), weshalb auf Artikel 13b verwiesen wird. Folglich dürfen die ComCom, das BAKOM und die Beauftragten Daten juristischer Personen gestützt auf eine hinreichende gesetzliche Grundlage bekanntgeben.

Personendaten juristischer Personen umfassen namentlich Informationen betreffend die Telekommunikationsunternehmen (Registrierungsdaten, finanzielle Informationen, Interkonktionsverträge), die Tarifdaten und die Dienste, die den Konsumentinnen und Konsumenten angeboten werden, die Leistungsdaten der Netze und Dienste (Dienstqualität, Verfügbarkeit) sowie Informationen zu Diensten, die beanstandet wurden (Art des Dienstes, Einzelheiten der Beanstandung) und andere. Diese Daten werden nicht als besonders schützenswert qualifiziert.

3. *Abschnitt*: Notkommunikation

Durch die Umstrukturierung der Bestimmungen im Bereich der Notkommunikation, soll ein neuer Abschnittstitel «Notkommunikation» den Abschnitt systematisch besser einreihen.

Art. 20 Grundsätze

Der Notrufdienst ist als Dienst der Anbieterinnen des öffentlichen Telefondienstes definiert, der es den Benutzerinnen und Benutzern ermöglicht, bei Gefahr für Leib, Leben, Gesundheit oder Eigentum die zuständige Alarmzentrale über einen Sprachanruf zu erreichen. Mit der Einführung des Zugangs über den Echtzeittext (*Real Time Text*, RTT; vgl. Art. 28a Abs. 6 FDV [verabschiedet, zum Zeitpunkt der Vernehmlassungseröffnung noch nicht in Kraft]) auf Verordnungsstufe, der im Rahmen des öffentlichen Telefondienstes von den Mobilfunkkonzessionärinnen sichergestellt werden muss, wird ein erster Schritt in Richtung einer modernen Ausgestaltung und einer barrierefreien Nutzung der Notdienste unternommen. Für eine grössere Flexibilität und um den Zugang weiter zukunftstauglicher und inklusiver ausgestalten zu können, soll der Begriff auf weitere mögliche Kommunikationsmittel und -wege ausgedehnt werden. Zu denken ist dabei an die Kontaktaufnahme über Textnachrichten oder die Videotelefonie. Das entspricht auch der internationalen Tendenz, insbesondere den Vorhaben in der EU.

In Artikel 20 sollen wie bis anhin sowohl der Grundsatz festgelegt, dass die die Anbieterinnen des öffentlichen Telefondienstes die Notkommunikation (mittels Sprachtelefonie) sicherzustellen haben, wie auch die Voraussetzungen, wann der Bundesrat die Notkommunikation auf weitere Fernmeldedienste und somit weitere Anbieterinnen von Fernmeldediensten ausdehnen kann. Das entspricht der geltenden Regelung, deren Prinzip unverändert übernommen wird.

Diese Grundsätze sind von allen Anbieterinnen des öffentlichen Telefondienstes sicherzustellen, beziehungsweise nach einer allfälligen Ausdehnung durch den Bundesrat auch von all denjenigen Anbieterinnen, welche den entsprechenden Fernmeldedienst anbieten. In erster Linie sind das die Anbieterinnen, welchen die konkrete Kommunikation aufbauen (bspw. den Sprachanruf aufbauen oder die Kommunikation initiieren). Es sind aber auch alle Anbieterinnen, die anderweitig an der Sicherstellung dieser Verbindung beteiligt sind. Das können Anbieterinnen sein, die den Transit der Kommunikation zwischen zwei anderen Anbieterinnen sicherstellen oder die Kommunikation bei den Zentralen terminieren.

Abs. 1

Absatz 1 hält fest, dass die Anbieterinnen des öffentlichen Telefondienstes die Notkommunikation sicherstellen müssen. Die Notkommunikation umfasst die Kommunikation über den öffentlichen Telefondienst vom Endgerät der Benutzenden bis hin zu den

von den Notdiensten oder den Hilfs- und Beratungsdiensten betriebenen zuständigen Zentralen, um deren Dienste für sich oder für Dritte in Anspruch nehmen zu können. Die Aufzählung, wann die Benutzenden die Zentralen erreichen können müssen, wurde aus der Bestimmung entfernt. Einerseits ist es dem Begriff Notkommunikation inhärent, dass es sich um eine aussergewöhnliche und zeitkritische Situation handeln muss, in der eine unmittelbare Gefahr für Leib, Leben, Gesundheit oder Eigentum besteht, in welcher eine schnelle Intervention durch Notdienste erforderlich ist. Andererseits war die Aufzählung bisher auch nicht komplett. Eine Intervention kann auch in einer Gefahrenlage für die Sicherheit der Allgemeinheit oder für die Umwelt erforderlich sein. Polizei und Sanität sind gerade auch in Situationen mit erhöhtem Gefahrenpotenzial präsent, wie etwa bei Grossanlässen. So rückt die Feuerwehr auch in Gefahrensituationen aus, in denen neben Menschen auch Tiere und allgemein die Natur bedroht sind, etwa bei Waldbränden oder Gewässerverschmutzungen.

Die Notdienste sorgen für die jederzeitige Bereitstellung der nötigen materiellen und personellen Ressourcen für eine zeitkritische Intervention unmittelbar am Ereignisort. Es handelt sich um die von den zuständigen Behörden anerkannten Organisationen der Polizei, der Feuerwehr und der Sanität, die über die jeweils dafür zur Verfügung gestellte Kurznummer nach Artikel 28 AEFV von den Benutzenden kontaktiert werden können.

Die Hilfs- und Beratungsdienste bieten den Anrufenden beratende Unterstützung in Situationen an, in denen keine unmittelbare Gefahrensituation besteht. Stellt sich im Gespräch heraus, dass umgehend Hilfe am Ereignisort benötigt wird, dann ist der entsprechende Notdienst zu kontaktieren, sei dies durch die Anrufenden selbst oder, falls dies nicht möglich ist, vom Hilfs- und Beratungsdienst. Die Hilfs- und Beratungsdienste sind nicht mit den notwendigen Ressourcen ausgestattet, um eine zeitkritische Intervention vor Ort vornehmen zu können. Bei diesen Diensten handelt es sich um die von den zuständigen Behörden anerkannten Organisationen, die über eine Kurznummer nach Artikel 28a AEFV (verabschiedet, zum Zeitpunkt der Vernehmlassungseröffnung noch nicht in Kraft) kontaktiert werden können (z. B. der Schweizerische Verband «Die Dargebotene Hand»). Wird ein Notdienst durch einen Hilfs- und Beratungsdienst kontaktiert, ist es zwingend notwendig, dass dem Notdienst insbesondere die Standortdaten zur Verfügung stehen. Die sogenannten Leistungsmerkmale – die Leitweglenkung (vgl. Art. 29 FDV), die Standortidentifikation (vgl. Art. 29 Abs. 1 FDV) und die Nutzung der geräteeigenen Ortungsfunktionen (vgl. Art. 29 Abs. 2 FDV), müssen jedoch aus technischen Gründen beim Aufbau der Kommunikation erfolgen, das heisst, bei der ursprünglichen Kontaktaufnahme mit dem Hilfs- und Beratungsdienst. Bei der nachträglichen Weiterleitung des Anrufs vom Hilfs- und Beratungsdienst an den Notdienst, kann die Standortidentifikation der Hilfesuchenden technisch nicht mehr erfolgen. In Bezug auf die Sicherstellung der Leistungsmerkmale sind die Hilfs- und Beratungsdienste daher den Notdiensten gleichgestellt.

Mit der zunehmenden technischen Komplexität der Netze und insbesondere auch der Endgeräte müssen die Anbieterinnen von Fernmeldediensten die Notkommunikation und vor allem auch die Leistungsmerkmale sicherstellen, soweit sie rechtlich und technisch dafür verantwortlich sind. Die Anbieterinnen von Fernmeldediensten haben gerade auf die Einstellungen und Funktionalitäten in den Endgeräten, die für das Absetzen einer Notkommunikation teilweise unabdingbare Voraussetzungen sind, keinen oder nur beschränkt Einfluss. Es sind oftmals Einstellungen, die durch die Nutzenden oder die Herstellerinnen vorgenommen werden müssen.

Abs. 2

In Absatz 2 wird, wie im geltenden Recht, festgehalten, dass die Anbieterinnen des öffentlichen Telefondienstes die beiden Leistungsmerkmale Leitweglenkung und Standortidentifikation sicherstellen müssen. Zusätzlich sollen die Anbieterinnen künftig zwecks Sicherstellung einer gewissen Redundanz im Ursprungsnetz eine minimale Rückfallebene sicherstellen müssen. Mit der Einführung einer minimalen Rückfallebene wird eine im Referenzmodell Notrufe⁵⁶ identifizierte Massnahme umgesetzt. Damit soll die Redundanz des Notkommunikationssystem zugunsten der Benutzerinnen und Benutzern sowie der Zentralen der Notdienste erhöht werden. Diese sind heute in der Regel redundant über zwei Anbieterinnen angeschlossen. Die redundante Erschliessung kann fernmelderechtlich nicht verbindlich festgelegt werden; die Zuständigkeit betreffend die Zentralen liegt bei den Kantonen. Die Pflicht zur Zweitanschliessung ergibt sich für die Notdienste jedoch ebenfalls aus dem Referenzmodell. Der Zweitanschluss und die minimale Rückfallebene führen insgesamt zur Steigerung der Verfügbarkeit, weil dadurch an zwei verschiedenen Stellen oder zu verschiedenen Zeitpunkten der Kommunikation die Redundanz des Netzes erhöht wird. Falls die Zustellung über das nach Artikel 20a Absatz 1 Buchstabe a betriebene Notkommunikationsnetz nicht möglich sein sollte, kann damit sichergestellt werden, dass eine Zustellung direkt über den zweiten Anschluss der zweiten Anbieterin erfolgt. Diese Rückfallebene von Absatz 2 muss am Anrufursprung und somit in den originierenden Netzen verankert werden. Es sind die originierenden Anbieterinnen, welche die Verfügbarkeit über den Erst- oder Hauptanschluss prüfen müssen. Die Zentralen der Hilfs- und Beratungsdienste, die über einen Zweitanschluss verfügen wollen oder müssen (z. B. aufgrund entsprechender kantonaler oder eigener Vorgaben der dienstbringenden Organisation), können in dem Falle auch von dieser erhöhten Redundanz profitieren.

Abs. 3

Absatz 3 enthält die Delegation an den Bundesrat, weitere Fernmeldedienste bezeichnen zu können, über welche die Grundsätze nach Absatz 1 und 2 auch sicherzustellen sind. Er macht dies nach Abwägung der Interessen der Bevölkerung und der Anbieterinnen sowie unter Berücksichtigung der technischen Entwicklung und der internationalen Harmonisierung. Die Fernmeldedienste müssen nach Buchstabe a öffentlich zugänglich sein und verbreitet genutzt werden. Buchstabe a entspricht somit dem bisherigen Absatz 3.

Nach Buchstabe b kann der Bundesrat Ausnahmen von der Sicherstellung der Pflichten nach Absatz 2 vorsehen und nach Buchstabe c, dass die Ortungsfunktionen von Endgeräten ohne ausdrückliche Zustimmung der Benutzerin oder des Benutzers genutzt werden dürfen. Beides ist in Absatz 2 der geltenden Bestimmung bereits so vorgesehen und wird lediglich neu strukturiert und umformuliert übernommen.

Art. 20a Systemaufgaben

Abs. 1

In Absatz 1 werden die übergeordneten Aufgaben – sogenannte Systemaufgaben – aufgeführt, mit denen die Notkommunikation sichergestellt werden muss. Es handelt sich dabei um übergeordnete, branchenweite Aufgaben, die im Gegensatz zu den Grundsätzen nach Artikel 20 nicht von allen Anbieterinnen von Fernmeldediensten

⁵⁶ UVEK und KKJPD (2022)

wahrgenommen werden, sondern von einer oder einigen Anbieterinnen für alle anderen Anbieterinnen. Damit soll insbesondere auch sichergestellt werden, dass einheitlich international oder national geltende Standards bei Technik, Informatik und Betrieb im Bereich der Systemaufgaben eingeführt oder übernommen werden. Das Prinzip orientiert sich an den in Artikel 37 des Eisenbahngesetzes vom 20. Dezember 1957⁵⁷ (EBG) festgelegten Systemaufgaben. Die Grundsätze nach Artikel 20 betreffen somit alle Anbieterinnen, die einen bestimmten Fernmeldedienst anbieten. Artikel 20a Absatz 1 hingegen betrifft nur eine Anbieterin oder unter Umständen einige wenige Anbieterinnen, welche die Systemaufgabe für die ganze Notkommunikationssystem und das ganze Notkommunikationswesen in der Schweiz wahrnehmen.

Bst. a

Der Betrieb eines ausschliesslich der Notkommunikation dienenden, jederzeit verfügbaren Netzes soll grundsätzlich mittels ESInet gewährleistet werden. Es handelt sich dabei um ein auf der Internetprotokoll-Familie basierendes, ausschliesslich dem Zweck der Notkommunikation dienendes, hochverfügbares Notkommunikationsnetz. Es stellt den Grundpfeiler für ein ausfallsicheres und zukunftstaugliches Notkommunikationssystem dar. Dabei handelt es sich um ein unverzichtbares Element der modernen Notfallkommunikationsinfrastruktur, da es die nötige Flexibilität und Skalierbarkeit für die unterschiedlichen Kommunikationskanäle und -technologien bietet, die in der Zukunft für Notkommunikation genutzt werden. Über das ESInet wird diese wie bis anhin schnell und zuverlässig an die richtige Zentrale der Notdienste weitergeleitet, basierend auf Faktoren wie dem Standort der hilfesuchenden Person oder der Art des Anrufs. Es sorgt somit dafür, dass die Einsatzkräfte schnell und zuverlässig an den Ereignisort gelangen können. Das ESInet ermöglicht den Übergang von traditionellen, sprachbasierten Notrufsystemen zu modernen IP-basierten Systemen, die auch die Notkommunikation über Multimedia-Dienste wie RTT und *Next Generation eCall* (NG eCall; modernisiertes, automatisches Notrufsystem für Fahrzeuge) unterstützen. Da es sich bei der Notfallkommunikation um ein kritisches Kommunikationsnetzwerk handelt, bietet das ESInet besondere Sicherheitsfunktionen, um zu garantieren, dass die Kommunikation sicher und ohne Unterbrechung weitergeleitet werden.

Bst. b

Die Architektur eines ESInet muss per se ausfallsicher ausgestaltet sein, um eine hohe Verfügbarkeit der darüber laufenden Kommunikation zu garantieren. Durch den redundanten Betrieb eines ESInet oder von Teilen davon durch eine Zweitanbieterin, wie dies als weitere Systemaufgabe in Buchstabe b vorgesehen ist, kann die Ausfallsicherheit und die Verfügbarkeit weiter erhöht werden, sofern dies notwendig erscheint.

Bst. c

Die Sicherstellung der Standortidentifikation durch den Betrieb eines entsprechenden Dienstes ist unverzichtbar, damit Notdienste vor Ort intervenieren und Hilfe leisten können. Der Dienst stellt die Übertragung und Zurverfügungstellung der Standortdaten der Anrufenden an die einsatzleistenden Notdienste sicher. Der Standortidentifikationsdienst wird heute durch die Grundversorgungskonzessionärin in Zusammenarbeit mit den anderen Anbieterinnen des öffentlichen Telefondienstes sichergestellt. Diese Verknüpfung ist historisch bedingt und kann mit dem geplanten Ansatzwechsel hin zu den

⁵⁷ SR 742.101

übergeordneten Systemaufgaben aufgelöst werden. Der Standortidentifikationsdienst ist Teil des ESInet.

Bst. d

Der Betrieb einer zentralen, jederzeit verfügbaren Koordinationsstelle für akute Notkommunikationsanliegen wird insbesondere von den Zentralen der Notdienste gewünscht, die sie vor allem bei drohender Überlastung kontaktieren und darüber Gegenmassnahmen koordinieren (z. B. bei durch Fehlfunktionen ausgelösten Anrufen auf die Zentralen, welche diese zu überlasten drohen).

Bst. e

Eine breite Palette von Endgeräten, insbesondere Smartphones oder auch Smartwatches, verfügen heute über ein System oder eine Funktion (z. B. mit Schock-/Sturzdetektion oder beim Auslösen von Airbags/Gurtstraffern), mit der eine Notkommunikation automatisch ausgelöst wird oder auch manuell ausgelöst werden kann (z. B. mehrmaliges Drücken der Seitentasten des Smartphones). Motorfahrzeuge müssen heute über ein solches System von Gesetzes wegen verfügen (NG eCall). Aktuell besteht weder für die Hersteller von Endgeräten oder Fahrzeugen noch für die Bevölkerung eine Möglichkeit, ein solches System oder eine solche Funktion unter realen Bedingungen zu testen und auf ihre Tauglichkeit zu prüfen. Auch die Anbieterinnen von Fernmeldediensten können keine oder nur unter eingeschränkten Bedingungen entsprechende Tests durchführen oder Dritten anbieten. Wer heute einen Test machen möchte, ist gezwungen, eine vermeintliche Notkommunikation auszulösen. Da immer mehr Endgeräte und Fahrzeuge mit solchen Systemen und Funktionen auf den Markt kommen stellen die Testanrufe durch die Bevölkerung und Hersteller für die Zentralen der Notdienste eine zunehmende Belastung dar. Es werden dadurch anderweitig dringend benötigte Ressourcen gebunden. Aus diesem Grund soll im Rahmen der Systemaufgaben der Betrieb einer realitätsgetreuen Test- und Integrationsplattform vorgesehen werden, die End-zu-End-Tests (von den Benutzerinnen und Benutzern, von denen die Notkommunikation ausgeht, bis zu den Testzentralen) für sämtliche derzeitigen wie auch zukünftigen Notruffunktionen ermöglicht. Für die Testplattform sind bei Bedarf auch die benötigten Adressierungselemente zur Verfügung zu stellen.

Bst. f

Damit die technischen und administrativen Vorschriften an die Systemaufgaben nach Absatz 1 und die technischen Anforderungen nach Absatz 2 überprüft werden können, muss eine zentrale Stelle die dafür nötigen Verkehrsdaten regelmässig erfassen, aufbereiten und dem BAKOM übertragen können. Diese Aufgabe kann die Koordinationsstelle nach Buchstabe d übernehmen.

Abs. 2

Die Anbieterinnen nach Artikel 20 müssen die technischen Anforderungen einhalten, die sich aus den Systemaufgaben zur Gewährleistung der Notkommunikation ergeben. Es handelt sich insbesondere um die Einhaltung der massgeblichen internationalen Normen und Standards. Absatz 2 richtet sich somit wiederum an alle Anbieterinnen des öffentlichen Telefondienstes. Damit die Notkommunikation insgesamt sichergestellt werden kann, müssen alle an der Kommunikation beteiligten Anbieterinnen bestimmte Anforderungen in ihren Netzen und während der Initiierung und Aufrechterhaltung der

Kommunikation sicherstellen. Die Anforderungen decken somit auch unterschiedliche Zeitpunkte in der Kommunikation ab, beziehungsweise sind jeweils zu einem bestimmten Zeitpunkt der Kommunikation relevant.

Abs. 3

Das BAKOM erlässt gestützt auf Absatz 3 die technischen und administrativen Vorschriften zu den Systemaufgaben nach Absatz 1 und legt die Anforderungen fest, welche die Anbieterinnen nach Artikel 20 erfüllen müssen, um die Verfügbarkeit der Systemaufgaben zu gewährleisten.

Art. 20b Verpflichtung zum Angebot von Systemaufgaben

Abs. 1

Gestützt auf Absatz 1 kann das BAKOM eine oder mehrere Anbieterinnen verpflichten, eine oder mehrere der Systemaufgaben nach Artikel 20a Absatz 1 sicherzustellen, wenn diese nicht bereits sichergestellt werden.

Abs. 2

Absatz 2 sieht vor, dass das BAKOM für eine Verpflichtung nach Absatz 1 ein Ausschreibungs- oder Einladungsverfahren durchführt, wenn mehrere Anbieterinnen für die Wahrnehmung einer Systemaufgabe in Frage kommen. Wie bei der Übertragung der Verwaltung von Adressierungselementen an Dritte nach Artikel 28a findet das Beschaffungsrecht keine Anwendung⁵⁸.

Abs. 3

Unter den in den Buchstaben a–c aufgeführten Voraussetzungen kann das BAKOM für die Wahrnehmung einer oder mehrere Systemaufgaben eine Anbieterin ohne Ausschreibungs- oder Einladungsverfahren bestimmen. Das kann bei fehlender Auswahl oder auch aus Zeitgründen der Fall sein. Möglicherweise zeigt sich auch von vornherein, dass ungenügendes Interesse an einer Wahrnehmung von Systemaufgaben besteht. Dies beispielsweise dann, wenn eine Umfrage in der Branche zeigt, dass keine oder nur eine Anbieterin interessiert ist oder dass ein Ausschreibungs- oder Einladungsverfahren zu keinen geeigneten Bewerbungen führen würde. Aufgrund der in Bezug auf die Sicherheit (Feuerwehr, Sanität und Polizei werden über die Notkommunikation kontaktiert) sensiblen Vergabe könnte es zudem angezeigt sein, sich auf in der Schweiz ansässige Anbieterinnen von Fernmeldediensten zu beschränken. Wie unter Kapitel [1.2.1](#) erwähnt, dürfte die Wahrnehmung dieser Aufgaben ausserdem ein bestimmtes Mass an Ressourcen und operativer Erfahrung zu Netzleistungen voraussetzen. Eine direkte Bestimmung ist entsprechend möglich, bei zeitlicher Dringlichkeit (vgl. Bst. a), wenn eine Marktbefragung aufzeigt, dass eine Ausschreibung nicht unter Wettbewerbsbedingungen ablaufen kann (vgl. Bst. b) und wenn bei einem Ausschreibungsverfahren kein Angebot eingereicht wird, das die Anforderungen der Ausschreibung erfüllt (vgl. Bst. c).

⁵⁸ BBI 2017 6559

Art. 20c Kostentragung

Abs. 1

Mit Artikel 20c Absatz 1 wird das heute auf Verordnungsstufe bestehende Prinzip betreffend die Kostentragung für den Betrieb eines Standortidentifikationsdienstes durch die Anbieterinnen von Fernmeldediensten auf Gesetzesstufe verankert. Die verrechenbaren Kosten der Systemaufgaben, wovon der Betrieb eines Standortidentifikationsdienstes nur einen Teil davon bildet, tragen alle nach Artikel 20 zur Notkommunikation verpflichteten Anbieterinnen.

Falls ein Ausschreibungs- oder Einladungsverfahren nach Artikel 20b Absatz 2 durchgeführt wird, ergeben sich die verrechenbaren Kosten vorab aus den Angaben der Anbieterin, welche den Zuschlag erhält. Bei einer Bestimmung nach Artikel 20b Absatz 3 dürften sich die verrechenbaren Kosten hingegen sinngemäss nach Massgabe der Grundsätze in Artikel 54 FDV ergeben. Eine entsprechende Regelung ist auf Verordnungsstufe vorzusehen. Ebenfalls auf Verordnungsstufe zu regeln sein wird die Abgeltung zwischen den Anbieterinnen. Diese Regelung soll sich grundsätzlich an den für den Standortidentifikationsdienst in Artikel 29b FDV bestehenden Bestimmungen orientieren.

Abs. 2

Die Benutzenden der Test- und Integrationsplattform nach Artikel 20a Absatz 1 Buchstabe e, welche beabsichtigen, diese Plattform für die Durchführung der in Artikel 20d vorgesehenen Tests zu nutzen, sollen einen angemessenen Anteil der verrechenbaren Kosten für die Wahrnehmung und Bereitstellung der Testplattform tragen. Somit sind, im Gegensatz zur Kostentragung nach Absatz 1, die Kosten nicht allein durch die Anbieterinnen zu tragen, welche nach Artikel 20 zur Notkommunikation verpflichtet sind.

Eine volle Kostentragung durch die Benutzenden der Test- und Integrationsplattform erscheint jedoch nicht angezeigt. Diese sind gemäss Artikel 20d für End-zu-End Tests zur Nutzung der Plattform verpflichtet. Die Tests kommen nicht nur den Benutzenden der Plattform zugute, sondern dem Gesamtsystem der Notkommunikation. Es sollen deshalb Anreize zum Testen geschaffen werden. Weiter fallen mit zunehmender Anzahl Tests für die einzelnen Benutzenden auch zunehmend tiefere Kosten an.

Art. 20d End-zu-End-Tests

End-zu-End Tests des Zugangs zur Notkommunikation nach Artikel 20 sind auf der Test- und Integrationsplattform nach Artikel 20a Absatz 1 Buchstabe e durchzuführen. Damit kann eine Entlastung des Notkommunikationssystems und des Notrufwesens sichergestellt werden. Einerseits dadurch, dass sie die zur Verfügung stehenden, begrenzten Ressourcen für tatsächliche Not-, Hilfs- und Beratungsfälle eingesetzt werden können und nicht durch Tests blockiert werden. Andererseits können die der Notkommunikation dienenden Systeme getestet und somit auch verbessert werden, was am Ende auch zu weniger vermeintlicher Notkommunikation führt (bspw. durch eine zu sensible Schockdetektion in einem Endgerät). Dies rechtfertigt eine Beteiligung an der Kostentragung durch die Testenden (vgl. vorangehende Ausführungen zu Art. 20c Abs. 2). Die Tests sind in Absprache mit der Koordinationsstelle nach Artikel 20a Absatz 1 Buchstabe d durchzuführen. Die Koordinationsstelle stellt somit die zentrale Ansprechstelle sowohl für die Anliegen der Zentralen wie der auch Hersteller von Endgeräten

oder Fahrzeugen mit entsprechenden Systemen für die Notkommunikation dar. Privatpersonen, die einzelne Tests zu eigenen Zwecken durchführen, sollen dabei grundsätzlich keine Kosten auferlegt werden. Auch entfällt in diesen Fällen aus Kapazitätsgründen eine Absprache mit der Koordinationsstelle.

Art. 20e Schutz der Integrität der Notkommunikation

Abs. 1

Absatz 1 verpflichtet die nach Artikel 20 zur Notkommunikation verpflichteten Anbieterinnen von Fernmeldediensten, Massnahmen gegen Gefährdungen der Integrität der Notkommunikation zu ergreifen. Damit soll weitmöglichst sichergestellt werden, dass die Systeme und Funktionen, die den Benutzenden eine Notkommunikation ermöglichen, die Integrität der Notkommunikation nicht gefährden.

Gefährdende Handlungen können namentlich vorliegen, wenn die Zentralen mit einer hohen Anzahl an vermeintlicher Notkommunikation belastet werden, so dass diese für tatsächliche Notfälle nicht mehr erreichbar sind. Ebenfalls ist an das Testen oder Inverkehrbringen von Endgeräten oder Fahrzeugen zu denken, welche aufgrund ihrer unausgereiften Funktionalität der integrierten Notkommunikationsfunktionen zur Überlastung des Notkommunikationsnetzes und der Zentralen führen können.

Die Integrität des Notkommunikationsnetzes muss dabei an sich gefährdet sein. Das kann aufgrund eines akuten, zeitlich beschränkten Vorfalls sein, wie eine massiv hohe Anzahl an Fehlkommunikation (i. S. von Fehlanrufen) in kurzer Zeit, welche die Kapazitäten ausschöpfen und daher die Erreichbarkeit der Zentralen gefährden. Darunter fallen insbesondere die Vorfälle, in denen die Anbieterinnen von Fernmeldediensten Massnahmen ergreifen und untereinander koordinieren müssen (vgl. Art. 28a Abs. 4 FDV [verabschiedet, zum Zeitpunkt der Vernehmlassungseröffnung noch nicht in Kraft]). Es können aber auch stetig wiederkehrende Fehlanrufe sein, deren Anzahl an sich die technische Kapazität und die Erreichbarkeit nicht zu tangieren vermag, jedoch zu einer ständigen Bindung von Ressourcen führt, weil sie immer wieder als vermeintliche Notkommunikation in Erscheinung treten. Zu denken ist an nicht oder mangelhaft getesteten Notkommunikationssysteme in Endgeräten, welche eine falsche Notrufkommunikation wiederkehrend auslösen. Dies ist beispielsweise der Fall, wenn Sensoren fälschlicherweise einen Sturz der Benutzenden des Endgeräts angeben. Eine solche Gefährdung ist weniger akut, belastet jedoch stetig die Ressourcen der Zentralen und gefährdet daher die Integrität der Notkommunikation. Es handelt sich um eine andauernde Gefährdung, welche beispielsweise durch ein Update der Software der Endgeräte behoben werden muss.

Mit der Regelung wird die auf Verordnungsebene vorgesehene Pflicht (vgl. Art. 28a Abs. 3 FDV [verabschiedet, zum Zeitpunkt der Vernehmlassungseröffnung noch nicht in Kraft]), die Notkommunikation vor einer hohen Anzahl an vermeintlichen Notfällen schützen zu müssen, auf Stufe Gesetz aufgenommen. Die Regelung wird dabei von akuten, die Erreichbarkeit gefährdenden, Ereignissen auf die Fälle ausgedehnt, die von der Anzahl her die Erreichbarkeit einer Zentrale zwar nicht zu gefährden vermögen, jedoch die Integrität durch stetige, fehlerhaft Notkommunikation untergraben und immer auch deren Ressourcen binden.

Einzelne Fehlanrufe von Einzelpersonen stellen dabei in der Regel keine Gefährdung des Notkommunikationssystems dar. Folglich ist beim Vorliegen vereinzelter Fehlanrufe grundsätzlich nicht von einer Gefährdung der Integrität auszugehen.

Abs. 2

Die Anbieterinnen stützen sich beim Ergreifen der Massnahmen insbesondere auf die Hinweise der Koordinationsstelle nach Artikel 20a Buchstabe d. Die Anbieterinnen ergreifen die Massnahmen umgehend und so lange wie nötig. Das ermöglicht ein schnelles Handeln bei den akuten Fällen, dient jedoch auch in den Fällen, in denen gewisse Endgeräte ein mangelhafte Notkommunikationsfunktionen aufweisen, welche vom Hersteller des Endgeräts über eine gewisse Dauer nicht behoben werden. Die Daten, welche von der Koordinationsstelle nach Artikel 20a Absatz 1 Buchstabe f erfasst werden, können insbesondere zur Identifikation fehlerhafter Notkommunikationsfunktionen herangezogen werden.

Abs. 3

Die Anbieterinnen von Fernmeldediensten dürfen Benutzerinnen und Benutzer zum Schutze der Integrität der Notkommunikation vom Netz trennen. Auch dies ist bereits im geltenden Recht auf Verordnungsstufe vorgesehen (vgl. Art. 28a Abs. 4). Eine Trennung ist grundsätzlich immer erst als letztmögliche Massnahme in Betracht zu ziehen. Sie ist insbesondere bei akuten Vorfällen angezeigt, um die Erreichbarkeit der zentralen sicherstellen zu können. Sie kann jedoch auch dann erfolgen, wenn Fehlalarme, sprich Fehlanrufe, durch mangelhafte Notkommunikationsfunktionen die Integrität der Notkommunikation stetig untergraben und der Hersteller diese Funktion auch nach mehrmaliger Information nicht nachträglich anpasst (z. B. im Rahmen eines Updates). Der Bundesrat soll auf Verordnungsstufe die entsprechenden technischen und organisatorischen Massnahmen festlegen können, welche die Anbieterinnen nach Absatz 1 ergreifen müssen und dürfen. Mit dieser Flexibilität kann der technologischen Entwicklung, aber vor allem auch den Bedürfnissen der Anbieterinnen, der Zentralen wie auch der Hersteller der Endgeräte angemessen Rechnung getragen werden.

Art. 29 Auskunftspflicht

Der Schutz der Fernmeldeinfrastrukturen vor Cyberbedrohungen und auch der Benutzerinnen und Benutzer im Umgang mit Fernmeldediensten ist ein grundlegendes Anliegen des Bundes und Hauptanliegen der vorliegenden Revision. Aus diesem Grund wird auch der Zweck des Fernmeldegesetzes dahingehend erweitert (vgl. Art. 1 Abs. 1 und Abs. 2 Bst. b und f). Artikel 29 konkretisiert die Pflichten der Inhaberinnen und Inhaber von Adressierungselementen, namentlich der Beauftragten nach Artikel 28a sowie die Rollen der im Bereich der Cybersicherheit tätigen Stellen.

Abs. 1

Diese Mitwirkungspflicht nach Absatz 1 stellt sicher, dass die Verwaltung von Adressierungselementen vollständig, korrekt und verlässlich erfolgt und dass der Bund seine Aufgaben im Bereich dieser Ressourcenzuteilung wahrnehmen kann.

Abs. 2

Neu regelt Absatz 2 die Zusammenarbeit im Bereich der Cybersicherheit. Anerkannte private und öffentliche Stellen, die für Aufgaben im Bereich der Cybersicherheit zuständig sind, können untereinander und mit den Beauftragten nach Artikel 28a kooperieren, um Gefährdungen durch Cyberbedrohungen zu erkennen und zu beurteilen. Mit den in Artikel 28a anvisierten Beauftragten ist insbesondere Switch als Registerbetreiberin der .ch-Domain gemeint, welche einen wesentlichen Beitrag zum Schutz der Domain-

Namen vor Cyberdrohungen leistet. Damit trägt das Gesetz der zunehmenden Bedeutung koordinierter Sicherheitsmassnahmen im Fernmeldebereich Rechnung und schafft eine rechtliche Grundlage für den strukturierten Informationsaustausch sowie gemeinsame Lagebeurteilungen. Die Vorschrift ermöglicht eine engere Zusammenarbeit zwischen staatlichen Akteuren und spezialisierten privaten Organisationen und stärkt damit die Resilienz der DNS-Infrastruktur. Es ist dabei unerlässlich, dass ein Informationsaustausch mit anderen an der Bekämpfung von Cyberisiken beteiligten Stellen erfolgen kann. Nur so kann ein effektiver Schutz der DNS-Infrastruktur wie auch der Benutzerinnen und Benutzer gewährleistet werden.

Der Begriff der privaten und öffentlichen Stellen umfasst Akteure, deren Tätigkeit ganz oder teilweise die Bekämpfung der Cyberkriminalität beinhaltet und die geeignet, qualitativ hochwertig und allgemein anerkannt sind.

Abs. 3

Absatz 3 ermächtigt den Bundesrat, die Kriterien festzulegen, nach denen private und öffentliche Stellen als für die Cybersicherheit zuständige Stellen anerkannt werden, mit welchen ein Informationsaustausch und eine Zusammenarbeit stattfinden darf. Diese Anerkennungs Voraussetzungen dienen der Qualitätssicherung sowie der Schaffung eines einheitlichen und transparenten Rahmens für die Aufgabenwahrnehmung der beteiligten Stellen. Sie stellen sicher, dass nur fachlich geeignete und organisatorisch verlässliche Akteure am Austausch sicherheitsrelevanter Informationen beteiligt sind.

Art. 30a Datenbearbeitung sowie Amts- und Rechtshilfe

Der neue Artikel 30a schafft einerseits eine datenschutzrechtliche Grundlage für Datenbearbeitungen im Zusammenhang mit der Erkennung, Analyse und Bewältigung von Cyberbedrohungen im Bereich der Adressierungselemente, insbesondere hinsichtlich der Sicherheit und des Funktionierens der DNS-Infrastruktur (vgl. Art. 28d Bst. a). Andererseits soll damit aber auch die Grundlage für die Zusammenarbeit mit spezialisierten Stellen im Bereich Cybersicherheit auf Gesetzesstufe verankert werden (vgl. Art. 28e Bst. c). Die Bestimmung ersetzt die frühere, wesentlich knappere Regelung, die lediglich auf die Anwendbarkeit der Artikel 13a und 13b verwies, und trägt damit der stark gestiegenen Bedeutung von Cybersicherheit im Fernmeldebereich Rechnung.

Dabei ist hervorzuheben, dass der überwiegende Teil der Analysen und Profilings, die zum Schutz vor Cyberbedrohungen durchgeführt werden, in der Regel nicht auf Personendaten im Sinne des DSG beruhen und daher keine besonders schützenswerte Personendaten umfassen. Vielmehr stützen sie sich auf technische Daten (Sachdaten), die keinen Bezug zu einer bestimmten Person aufweisen. So etwa technische Daten von Fernmeldeinfrastrukturen, Merkmale von Schadsoftware oder typische Vorgehensweisen bei Cyberangriffen. Zudem betreffen zahlreiche Daten Konstellationen, bei denen eine Identifikation von im Internet agierenden Einheiten faktisch nicht möglich oder zur Erreichung des Schutzes der Benutzerinnen und Benutzer beziehungsweise der DNS-Infrastrukturen nicht erforderlich ist. Schliesslich handelt es sich häufig um Daten, die einen Bezug zu einer juristischen Person aufweisen, etwa zu Herstellern von Fernmeldeanlagen oder -infrastrukturen.

Abs. 1

Artikel 30a Absatz 1 erlaubt dem BAKOM sowie den nach Artikel 28a beauftragten Stellen, zur Erfüllung der gesetzlich vorgesehenen Aufgaben Profilings durchzuführen

und dabei bei Bedarf auch besonders schützenswerte Personendaten zu bearbeiten. Diese Aufgaben ergeben sich aus Artikel 28d Buchstabe a (Sicherstellung der Sicherheit und Verfügbarkeit der DNS-Infrastruktur) sowie Artikel 28e Buchstabe c (Massnahmen gegen widerrechtliche oder ordnungswidrige Nutzung von Domain-Namen und Zusammenarbeit mit spezialisierten Stellen im Bereich Cybersicherheit). Mit den in Artikel 28a anvisierten Beauftragten ist insbesondere Switch als Registerbetreiberin der .ch domain gemeint, welche einen wesentlichen Beitrag zum Schutz der Domain-Namen vor Cyberdrohungen leistet und deshalb auch die notwendigen Personendaten bearbeiten dürfen soll.

Nach Artikel 34 Absatz 2 DSG dürfen besonders schützenswerte Personendaten sowie Profilings nur bearbeitet werden, wenn hierfür eine ausdrückliche gesetzliche Grundlage besteht. Artikel 30a Absatz 1 schafft diese Grundlage und ermöglicht es dem BAKOM und den nach Artikel 28a Beauftragten auch verdeckte Analysen vorzunehmen und biometrische Daten sowie Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen zu bearbeiten, soweit dies für den Schutz vor Cyberbedrohungen erforderlich ist.

Zwar sind die dabei verwendeten Daten nicht in jedem Fall besonders schützenswert, doch kann ihre algorithmische Auswertung oder ihr Abgleich mit weiteren Informationen – etwa zur Feststellung der Identität der Halterin oder des Halters eines Domain-Namens – bereits ein Profiling darstellen. In bestimmten Konstellationen kann zudem die Bearbeitung besonders schützenswerter Daten notwendig sein, um die Resilienz der DNS-Infrastrukturen und den Schutz vor Cyberbedrohungen wirksam zu gewährleisten. So können etwa einschlägige Vorstrafen wertvolle Hinweise für die Erkennung von Risikoprofilen liefern. Der Zugang zu solchen Informationen trägt wesentlich dazu bei, die Herkunft gezielter Bedrohungen wie «*Distributed-Denial-of-Service*»-Angriffe (DDoS), Phishing oder die Verbreitung von Malware zu erkennen und zuzuordnen. In Einzelfällen kann auch die in Netzwerken zunehmend eingesetzte biometrische Identifikation erforderlich sein, um Handlungen einer bestimmten Person zuzuweisen oder eine unzulässige Nutzung von Domain-Namen festzustellen, die auf cyberkriminelle Aktivitäten hinweisen kann.

Die Bekämpfung von mithilfe von Domain-Namen verübter Cyberkriminalität ist ein gutes Beispiel für die Bearbeitung von Personendaten nach diesem Absatz. Gestützt auf Artikel 28e Buchstabe c ermöglicht Artikel 25 Absatz 1^{bis} bis 1^{quater} VID zum Beispiel der Registerbetreiberin von .ch, einen Domain-Namen bei Verdacht auf eine Nutzung in unrechtmässiger Weise oder zu einem unrechtmässigen Zweck nicht zu aktivieren, da die Aktivierung, die die effektive Nutzung des Domain-Namens ermöglicht, erst nach einer erneuten Identifikation der Halterin oder des Halters innerhalb von 30 Tagen erfolgt. Dieser Prozess der aufgeschobenen Nutzung von Domain-Namen (*Deferred Delegation*) basiert auf einem Bewertungsalgorithmus (*Scoring*) der Registerbetreiberin, der die Registrierungsdaten überprüft und beurteilt, ob die gesuchstellende Person korrekte Angaben zu ihrer Identität gemacht hat. Statistische und historische Daten der Registerbetreiberin, Informationen von *Computer Emergency Response Teams* (CERT) und Dritten, die an der Bekämpfung von Cyberkriminalität beteiligt sind, sowie wissenschaftliche Arbeiten dienen als Grundlage für die Analyse, um so eine fundierte Vorhersage hinsichtlich der künftigen Nutzung eines Domain-Namens zu treffen.

Vor diesem Hintergrund und zur effizienten Bekämpfung wachsender Bedrohungen im Bereich der Cybersicherheit ermächtigt diese Rechtsgrundlage die zuständigen Behörden zum gezielten und verhältnismässigen Einsatz fortschrittlicher Technologien, einschliesslich künstlicher Intelligenz. Dadurch soll insbesondere die automatisierte

Analyse digitaler Verhaltensweisen ermöglicht werden, bei denen ein Verdacht auf missbräuchliche oder strafbare Aktivitäten besteht, um im digitalen Raum mittels Domain-Namen begangene Angriffe zu erkennen, zu verhüten und zu verhindern.

Abs. 2

Die Weitergabe der bearbeiteten Daten sowie der Ergebnisse von Profilings an Schweizer Behörden sowie an private und öffentliche Stellen sollen unter spezifischen Umständen ermöglicht werden. Damit wird ein strukturierter Informationsaustausch geschaffen, der erforderlich ist, um Cyberbedrohungen umfassend zu erkennen, zu analysieren und zu entschärfen. Die Weitergabe ist jedoch nur zulässig, wenn die empfangende Behörde selbst über eine hinreichende gesetzliche Grundlage verfügt – was eine wichtige datenschutzrechtliche Schranke darstellt und den Grundsatz der Zweckbindung sicherstellt. Es handelt sich dabei um Behörden, die ebenfalls im Bereich der Cybersicherheit Aufgaben erfüllen, wie namentlich das BACS, fedpol oder das Staatssekretariat für Sicherheitspolitik (SEPOS).

Abs. 3

Der Bundesrat wird ermächtigt, die Einzelheiten der Bearbeitung besonders schützenswerter Personendaten sowie der Durchführung von Profilings zu regeln. Er kann insbesondere Anforderungen an die Datensicherheit, die Verfahrensabläufe, die Protokollierung, die Lösch- und Aufbewahrungsfristen sowie an die Zuständigkeiten festlegen. Diese Delegation ermöglicht eine flexible und technologieneutrale Ausgestaltung, welche der raschen Entwicklung im Bereich der Cybersicherheit Rechnung trägt.

Sie stützt sich auf Artikel 34 Absatz 3 DSG, wonach für die Bearbeitung besonders schützenswerter Personendaten oder die Durchführung von Profilings in bestimmten Fällen eine Grundlage in einem Gesetz im materiellen Sinn ausreicht. Der Bundesrat hat dabei sicherzustellen, dass solche Bearbeitungen keine besonderen Risiken für die Grundrechte der betroffenen Personen bergen. Es handelt sich um Datenbearbeitungen, die für die Erfüllung einer gesetzlichen Aufgabe unerlässlich sind (vgl. Art. 34 Abs. 3 Bst. a DSG) und deren Zweck – der Schutz der betroffenen Ressourcen – für sich genommen kein besonderes Risiko für die Grundrechte der Benutzerinnen und Benutzer darstellt (vgl. Art. 34 Abs. 3 Bst. b DSG).

Da es nicht möglich ist, im Voraus alle Instrumente zu definieren, die zur Bekämpfung von Cyberkriminalität erforderlich sein können – etwa zur Erkennung, Verhütung, Verhinderung oder Verfolgung von Straftaten, die im digitalen Raum mithilfe von Domain-Namen begangen werden –, obliegt es dem Bundesrat, die Durchführung von Profilings und die Bearbeitung besonders schützenswerter Daten im Bedarfsfall zu konkretisieren. Dabei hat er die besonderen Eigenschaften der eingesetzten Instrumente zu berücksichtigen, wie sie in der Fernmeldegesetzgebung etwa im Rahmen des Prozesses der aufgeschobenen Nutzung von Domain-Namen der VID vorgesehen sind oder künftig vorgesehen werden können. Dazu gehört namentlich die Festlegung der betroffenen besonders schützenswerten Daten sowie der Anforderungen an deren technischen und organisatorischen Sicherheit.

Abs. 4

Absatz 4 stellt klar, dass die allgemeinen Bestimmungen über Datenbearbeitung (vgl. Art. 13a) und Amtshilfe (vgl. Art. 13b) auch auf die in Artikel 30a geregelten Datenbearbeitungen und deren Bekanntgabe an schweizerische oder ausländische Behörden

Anwendung finden. Dies gewährleistet eine einheitliche Handhabung im gesamten Datenschutz- und Amtshilferegime des Fernmelderechts.

5. Kapitel: Fernmeldeanlagen

Im Rahmen der vorliegenden Revision soll die Systematik im 5. Kapitel (Fernmeldeanlagen) leicht geändert werden. Dabei soll künftig die Reihenfolge der geltenden Artikel 32a und 32b getauscht werden. In Artikel 32b soll dabei ebenfalls der geltende Artikel 34 Absatz 1^{ter} überführt werden. Zusätzlich soll der geltende Artikel 34 in zwei Artikel aufgetrennt werden und der bestehende Artikel 34a soll zu Artikel 34b werden. Diese Bestimmungen sollen zugunsten einer verbesserten öffentlichen Sicherheit ebenfalls geändert werden.

Art. 32a Verbot störender Funkanlagen sowie anderen Anlagen und Vorrichtungen

Abs. 1

Diese Bestimmung entspricht grösstenteils dem geltenden Absatz 1 von Artikel 32b, ergänzt mit dem Begriff «Anlagen». Unter «Anlagen» sind Geräte, Leitungen oder Einrichtungen zu verstehen, die keine Informationen im fernmeldetechnischen Sinn (vgl. Art. 3 Bst. c und d) übertragen, dennoch aber das Frequenzspektrum nutzen (bspw. Störsender). Zudem wird im deutschen und italienischen Text ein Übersetzungsfehler korrigiert: Es sollte Funkanlagen statt Fernmeldeanlagen heissen.

Abs. 2

Neben den bisher geregelten störenden Anlagen und Vorrichtungen, die dazu bestimmt sind, absichtlich den Fernmeldeverkehr zu stören, sind weitere Konstellationen denkbar, die eine ähnliche Wirkung haben und deshalb ins Gesetz aufgenommen werden sollen.

Einerseits geht es um Vorrichtungen, die ein Zielgerät durch Zerstörung derer Elektronik ausschalten können. Technologische Entwicklungen haben gezeigt, dass nicht nur Anlagen wie Störsender die Kommunikation stören respektive verhindern können, sondern beispielsweise auch ein elektromagnetischer Impulsgenerator (EIMP-Generator), der eine ähnliche Funktion haben kann: Ein solcher Generator kann durch eine kurze intensive Sendung elektromagnetischer Impulse Elektronikteile eines Gerätes, zum Beispiel einer Alarmanlage, zerstören und dadurch gleichzeitig den Fernmeldeverkehr im weiteren Sinne beeinträchtigen. Im Interesse der öffentlichen Sicherheit soll diese Technologie als Sonderelektronik den schweizerischen Sicherheitsbehörden zur Wahrung der öffentlichen Sicherheit ebenfalls zugänglich gemacht werden (vgl. Bst. a).

Andererseits geht es um konforme Anlagen, die so konfiguriert werden können, dass sie die Kommunikation einer gleichartigen Anlage hemmen, das heisst vorübergehend verhindern, oder unterbrechen. Als Beispiel kann ein drahtloses Netzwerk (*Wireless Fidelity*, WiFi) aufgeführt werden, das absichtlich mit einem anderen WiFi kollidiert, um dadurch die Kommunikation zu hemmen oder zu unterbrechen. Das ist als eine Art *Hacking* zu betrachten. Dabei erteilt ein WiFi dem anderen sinnbildlich den «Befehl», nicht zu kommunizieren (vgl. Bst. b).

Es liegt somit keine Störung im Sinne des Fernmelderechts vor, aber die Kommunikation wird dennoch verhindert.

Abs. 3

Dieses Verbot nach Absatz 1 gilt nicht für Anlagen und Vorrichtungen zur Wahrung der öffentlichen Sicherheit (vgl. Art. 32b). In diesem Sinn ist auch Artikel 32b vorbehalten.

Art. 32b Fernmeldeanlagen sowie andere Anlagen und Vorrichtungen zur Wahrung der öffentlichen Sicherheit

Abs. 1

Der Einleitungssatz entspricht grösstenteils dem geltenden Absatz 1 von Artikel 32a mit der analogen Ergänzung von Anlagen (vgl. dazu die Ausführungen zu Art. 32a).

Abs. 2

Die Auflistung der Behörden, die störende Anlagen einsetzen können, entspricht den geltenden Buchstaben a bis d von Artikel 34 Absatz 1^{ter}.

Abs. 3

Diese Bestimmung zielt darauf ab, die Mitwirkungspflichten der gesuchstellenden Personen für eine effiziente Regulierung der Sonderelektronik, die von Behörden im Sinne von Absatz 1 für die Erfüllung ihrer Aufgaben benötigt werden, zu schaffen.

Für die Regulierung von Sonderelektronik müssen die notwendigen Informationen (v.a. technischen Unterlagen) von den gesuchstellenden Personen dem BAKOM bereitgestellt werden. Diese beinhalten oftmals Geschäftsgeheimnisse und sind vertraulich zu behandeln. Bei den gesuchstellenden Personen handelt es sich überwiegend um ausländische Unternehmen, die selbst den Behörden die erwähnten Unterlagen kaum herausgeben. Mit dieser Bestimmung soll den gesuchstellenden Personen die vertrauliche Behandlung der Informationen zugesichert werden. Als vertraulich zu klassifizieren sind zudem sowohl die fraglichen Anlagen und Vorrichtungen (inkl. Zulassung) als auch Informationen über die Behörden, welche diese im Interesse der öffentlichen Sicherheit mit einer Betriebsbewilligung nutzen. Damit soll das Risiko, dass ausländische Nachrichtendienste, kriminelle Organisationen oder Einzelpersonen diese sicherheitsrelevanten Informationen zum Nachteil der öffentlichen Sicherheit nutzen können, verhindert werden. Das BAKOM stellt dem beschränkten Kreis der Behörden nach Artikel 32b Absatz 1 eine Liste der Personen, die über eine Bewilligung für das Herstellen, Importieren und Bereitstellen auf dem Markt von Sonderelektronik innehaben, sowie eine Liste der zugelassenen Anlagen zur Verfügung (vgl. dazu Art. 27 Abs. 3 und Abs. 4 der FAV).

Die betroffenen Schweizer Behörden nach Absatz 1 sind zudem aufgrund der geopolitischen Situation immer mehr auf solche Anlagen angewiesen. Der politische Druck für die Betriebsbewilligungen von Sonderelektronik ist beträchtlich, zu nennen sind namentlich internationale Veranstaltungen und Konferenzen wie das *World Economic Forum* WEF in Davos, multinationale Friedensgespräche, wie die Ukraine Recovery Conference (Lugano) oder die Konferenz zum Frieden in der Ukraine (Bürgenstock). Bei solchen Veranstaltungen mit grossen Sicherheitsanforderungen braucht es beispielsweise eine wirksame Drohnenabwehr, welche ebenfalls unter den Begriff Sonderelektronik fällt. Um entsprechenden Gefahren entgegen wirken zu können, benötigen die Polizei und die Armee Anlagen und Vorrichtungen aus dem Bereich der Sonderelektronik.

Aus diesen Gründen sind die von den gesuchstellenden Personen eingereichten Informationen, die Anlagen und Vorrichtungen sowie die Informationen über die mit einer Betriebsbewilligungen ausgestatteten Behörden vertraulich zu klassifizieren, damit die Informationen vollständig eingereicht werden, das BAKOM folglich die notwendigen Informationen erhält und die betroffenen Schweizer Behörden diese Anlagen im Interesse der öffentlichen Sicherheit rechtmässig, sprich mit einer Bewilligung des BAKOM, einsetzen können. Überdies kann damit die Qualität der notwendigen Informationen sichergestellt werden wie auch der Aufwand, bis die Schweizer Behörden diese Anlagen benützen können, verringert werden.

Art. 34 Störung

Abs. 1

Das Erstellen und Betreiben von Fernmeldeanlagen mit dem Ziel, den Fernmeldeverkehr oder den Rundfunk zu stören oder zu verhindern, soll als verwaltungsrechtliches Verbot aufgenommen werden (vgl. auch Art. 52 Abs. 1 Bst. j).

Abs. 2

Das BAKOM ist für die Behebung von Störungen im Bereich des Fernmeldeverkehrs und des Rundfunks zuständig. Zu diesem Zweck betreibt es eine spezialisierte Messinfrastruktur, um Störungen des Funkfrequenzspektrums rasch lokalisieren zu können. Letztere werden nicht nur von Fernmeldeanlagen verursacht, sondern auch von elektrischen Geräten wie Haartrocknern, LED-Lampen, Aufzügen, Belüftungs- und Klimaanlage oder Anzeigetafeln mit mehreren Bildschirmen, um nur einige Beispiele zu nennen. Zur Vermeidung und zur Lokalisierung von Störungen ist es erforderlich, dass das BAKOM bei elektrischen Stark- oder Schwachstromanlagen die gleichen Massnahmen ergreifen kann und das gleiche Zugangsrecht besitzt wie bei Fernmeldeanlagen. Diese Kompetenzen des BAKOM sind derzeit auf Stufe Bundesratsverordnung in der Verordnung vom 25. November 2015⁵⁹ über elektromagnetische Verträglichkeit (VEMV) verankert; sie sollen jedoch im Rahmen der vorliegenden Revision in eine formell rechtliche Grundlage auf Gesetzesstufe überführt werden (vgl. Abs. 2). Bei einer allfälligen Störung des Spektrums durch Anlagen des Stromübertragungs- und -verteilungsnetzes oder durch jene von Eisenbahnen oder Trolleybussen hört das BAKOM die betroffenen Parteien an, erlässt gegebenenfalls Massnahmen und bestimmt den Zeitplan für deren Umsetzung sowie die Kostenaufteilung, wobei es die sich gegenüberstehenden Interessen von Fall zu Fall abwägt. Gegen den Erlass einer entsprechenden Verfügung kann Beschwerde geführt werden.

Weiter geht es nicht nur um die Störung des Frequenzspektrums, sondern auch um die Verhinderung der Kommunikation, weshalb die Bestimmung mit «verhindert» (vgl. dazu die Ausführungen zu Art. 32a Abs. 2) zu ergänzen ist.

Es ist darauf hinzuweisen, dass die Betreiberin oder der Betreiber eine natürliche wie auch juristische Personen sein kann.

⁵⁹ SR 734.5

Abs. 3 und 4

Diese beiden Absätze entsprechen den geltenden Absätzen 1^{bis} und 1^{quater} mit kleinen redaktionellen Anpassungen.

Art. 34a Lokalisierung von Störungen

Der geltende Artikel 34a wird aufgrund der geänderten Systematik neu zu Artikel 34b und wird dabei redaktionell präzisiert, ohne, dass materielle Anpassungen vorgenommen werden.

Abs. 1

In der bisherigen deutschen Fassung von Artikel 34 Absatz 2 ist dem BAKOM «Zutritt zu allen Fernmeldeanlagen» zu gewähren. In der Praxis hat sich herausgestellt, dass diese Formulierung nicht präzise genug ist, denn sie umfasst den Zugang zu Fernmeldeanlagen beispielsweise in Fahrzeugen nicht. Aus diesem Grund ist Zutritt durch Zugang zu ersetzen. Betreffend die Ergänzungen zu den Stark- und Schwachstromanlagen wird auf die Ausführungen zu Artikel 34 Absatz 2 verwiesen.

Mit dem Aufkommen von 5G und zukünftigen neuen Technologien (6G/7G) stellen Antennen mit steuerbarem Strahl (*Beamforming*) neue Herausforderungen für die Erkennung von Störungen dar.

Adaptive Antennen senden die Funksignale nicht mehr konstant in eine Richtung, wie dies bei konventionellen Antennen der Fall ist. Stattdessen fokussieren sie die Strahlung dorthin, wo sich das verbundene Mobiltelefon befindet, und reduzieren sie in anderen Richtungen. Adaptive Antennen können folglich nicht synchron mit ihrer gesamten Leistung in jede denkbare Richtung strahlen, sondern teilen ihre Leistung auf räumlich unterschiedliche Ziele auf. Die neuen *Beamforming*-Antennen stellen folglich eine Herausforderung für die Suche nach dem Ursprung einer Störung dar.

Die Mobilfunkanlagen, welche über adaptive Antennenmodule verfügen, werden durch sogenannte umhüllende Antennendiagramme spezifiziert. Das heisst, dass alle möglichen *Beams* (Senderrichtungen) in ein 3D-Diagramm einbezogen werden und davon wird die maximal umhüllende Kontur abgespeichert. Im Betrieb wird nun je nach Position der Endgeräte der bestmögliche Beam benutzt, um die Daten zu senden. Dabei kann die Senderichtung im Millisekunden-Takt geändert werden.

Für die Störungslokalisierung muss das BAKOM wissen, welcher *Beam* an einem genauen Zeitpunkt aktiv ist (bspw. bei sporadisch immer wieder auftretenden Störungen). Dann können Rückschlüsse zu erfolgten Störungen gemacht werden.

Um wiederkehrende Störsignale im Mobilfunkbereich zeitlich und örtlich lokalisieren und einer spezifischen Fernmeldeanlage zuweisen zu können, ist es zwingend erforderlich, dass das BAKOM von den Anbieterinnen, Eigentümerinnen oder Betreiberinnen Daten über die Entwicklung der Strahlungsdiagramme über einen bestimmten Zeitraum oder zu einem bestimmten Zeitpunkt (insb. zu den Abstrahlungseigenschaften und den Abstrahlungseinstellungen der betroffenen Anlage) anfordern kann. Dies gewährleistet eine genaue Rekonstruktion der Bedingungen, unter denen eine Störung aufgetreten ist, wobei die Ursache auch bei der Mobilfunkbetreiberin selbst gefunden werden kann.

Abs. 2 und 3

Das BAKOM ist für die Lokalisierung von Störungen des Frequenzspektrums zuständig. Von hoher und aktueller Relevanz für das BAKOM sind Störungen der globalen Navigationssatellitensysteme (*Global Navigation Satellite System* [GNSS], wie z.B. GPS, GLONASS, Galileo und Beidou). GNSS-Signale sind unabdinglich unter anderem beim Instrumentenflug (Flug ohne Sicht) und bei der Zeitsynchronisation von wichtigen Diensten wie Strom- und Mobilfunknetzen sowie Börsenaktivitäten zentral. Die GNSS-Signale der Satelliten sind auf der Erde sehr schwach und daher in einer erhöhten Masse störanfällig. Bereits im Jahre 2022 wurden dem BAKOM diesbezüglich Zwischenfälle der Rettungsflugwacht sowie der allgemeinen Zivilluftfahrt gemeldet, bei welchen die Navigationssysteme aufgrund von Störungen des Funkspektrums ausgefallen sind. Derartige Störungsmeldungen gehen beim BAKOM weiterhin regelmässig ein.

Um möglichst viele potenzielle Störquellen auffinden zu können, hat das BAKOM Feldmessungen entlang von Strassen durchgeführt. Dadurch konnten unabsichtliche Störungen (z.B. mangelhaftes elektrisches oder elektronisches Bauteil im Fahrzeug) wie auch absichtliche Störungen durch den Betrieb von verbotenen Störsendern (vgl. Art. 32a, wonach bereits deren Besitz verboten ist) gemessen werden. So wurden an drei verschiedenen Orten entlang Autobahnen bei kontinuierlichen Messungen im Frequenzspektrum innerhalb von 15 bis 30 Tagen fast täglich starke Störungen festgestellt, die das GNSS-Signal potenziell zu stören vermögen.

Zwar können bei Feldmessungen Störungen festgestellt werden, jedoch können die fehlbaren Fahrzeuge aufgrund der kurzen Durchfahrtszeit nicht von blossen Auge identifiziert werden. Deshalb soll eine automatisiert optische Erfassung von dem betreffenden Fahrzeug erfolgen. Dementsprechend wird die automatisiert optische Erfassung bei Vorhandensein eines störungsverursachenden Signals - und nur in diesem Fall - ausgelöst.

Kann aufgrund von Feldmessungen eine gewisse Regelmässigkeit eines betriebenen Störsenders festgestellt werden, wird eine Kontrolle mit einer Drittbehörde durchgeführt. Wird vor Ort die typische Signatur eines Störsenders im Frequenzspektrum festgestellt, erfolgt die optische Erfassung des Fahrzeugs (v. a. Kontrollschild) und das BAKOM informiert die anwesende, zuständige kantonale Polizeibehörde, das Grenzwachkorps oder allenfalls fedpol, um das betreffende Fahrzeug anzuhalten, damit das BAKOM die Anwesenheit eines Störsenders festzustellen kann. Die Kontrolle wird von den Mitarbeitenden des BAKOM durchgeführt.

Eine Kooperation mit den Polizeibehörden oder dem Grenzwachkorps ist dabei aus mehreren Gründen notwendig:

- Die Polizei kann Fahrzeuge - bei unkooperativem Verhalten - auch ohne Einwilligung durchsuchen, wenn unter anderem zu vermuten ist, dass zu beschlagnahmende Gegenstände gefunden werden (vgl. Art. 249 StPO);
- Zum Schutz der Mitarbeitenden des BAKOM, da Störsender insbesondere für kriminellen Aktivitäten und somit durch potenzielle Straftäter und Straftäterinnen eingesetzt werden;
- Zudem verringert eine zeitnahe Feststellung und Beschlagnahme eines Störsenders vor Ort das Risiko, dass dieser beiseitegeschafft wird.

Es findet folglich keine systematische oder gar grossflächige Erfassung vorbeifahrender Fahrzeuge statt. Es wird auch keine verwaltungspolizeiliche Informationsbeschaffungsmassnahme bezweckt (ähnlich jener der automatisierten Fahrzeugfahndung und Verkehrsüberwachung), sondern die konkrete Umsetzung eines Leistungsauftrags des BAKOM im Rahmen seiner Kompetenzen.

Als Anwendungsfälle kommen grundsätzlich zwei Arten von Störungen in Frage: unabsichtliche und absichtliche Störungen.

Durch das oben umschriebene Vorgehen werden datenschutzrechtliche Bestimmungen tangiert. Bei Messungen von Funksignalen liegt zwar noch keine Bearbeitung von Personendaten vor, da diese nicht personenbezogen sind.

Sobald aber eine automatisiert optische Erfassung von Fahrzeugen bei einer eindeutigen Verletzung des Funkspektrums ausgelöst wird, die erkennbare datenrelevante Inhalte zeigt, ist eine Zuordnung grundsätzlich möglich und somit ein allfälliger Personenbezug gegeben. Neben Datum, Zeit und Ort des Ereignisses soll mit der automatisiert optischen Erfassung jeweils Fahrzeugtyp, -marke, Kontrollschild und allenfalls Fahrzeugfarbe erhoben werden.

Das BAKOM ist gehalten, alle technischen Massnahmen zu ergreifen, um die Erfassung von unerwünschten Personendaten gänzlich auszuschliessen oder entsprechend auf einen tiefst möglichen Stand zu minimieren. Ebenfalls sieht das BAKOM vor, bei der künftigen Beschaffung des Systems, die spezifischen Datenschutzbestimmungen für dieses Vorhaben in den Beschaffungsunterlagen eindeutig als Kriterium zur Vergabe festzuhalten.

Die Ursache der Störung spielt eine grosse Rolle, da je nach deren Qualifikation (absichtliche oder unabsichtliche Störung) unterschiedliche Rechtsverfahren gestützt auf einer anderen Rechtsgrundlage zur Anwendung gelangen und damit unterschiedliche rechtliche Konsequenzen haben. Dies hat Auswirkungen auf den zu ergreifenden Schutz der Personendaten und damit einen Einfluss auf das zu beschaffende System.

Aktuelle Erkenntnisse zeigen, dass eine Reihe von Fahrzeugen unabsichtliche breitbandige Störungen verursachen, die den Empfang von GNSS-Signalen beeinträchtigen können. Wenn eine Häufung von solchen unabsichtlichen Störsignalen bei bestimmten Fahrzeugtypen festgestellt werden kann, kann im Nachgang eine Konformitätsprüfung in einem Verwaltungsverfahren gemäss dem Bundesgesetz vom 20. Dezember 1968⁶⁰ über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz; VwVG) gegen die verantwortliche Person durchgeführt werden. Ein solches ist insbesondere gegen die Inverkehrbringerin aber auch gegen die Halterin oder den Halter möglich, so beispielsweise beim nachträglichen Einbau elektrischer Geräte oder beim späteren Austauschen des Autoradios.

Einfache Bildaufnahmen von Fahrzeuginsassinnen und -insassen sowie von weiteren personenbezogenen Merkmalen bei Fahrzeugen (natürliche und/oder juristische Personen) stellen bei unabsichtlichen Störungen keine besonders schützenswerten Personendaten dar. Es handelt sich zwar um ein Verwaltungsverfahren, nicht aber um ein Verwaltungsstraf- oder Strafverfahren. Die erhobenen Personendaten fallen damit nicht unter Artikel 5 Buchstabe c DSGVO.

⁶⁰ SR 172.021

Stellt das BAKOM jedoch fest, dass eine absichtliche Störung durch einen Störsender im Fahrzeug (vgl. Art. 32a) verursacht worden ist, so ist - nach der Kontrolle des Fahrzeugs - ein Verwaltungsstrafverfahren gemäss dem Bundesgesetz vom 22. März 1974⁶¹ über das Verwaltungsstrafrecht (VStrR) gegen den Fahrer oder die Fahrerin zu eröffnen. Ein Verfahren gegenüber der Importeurin des Fahrzeuges erübrigt sich, da ein Störsender nicht zur Ausstattung gehört.

Es ist zu klären, ob die Daten betreffend die automatisiert optisch erfassten Fahrzeuge bei der Vermutung des Mitführens eines Störsenders besonders schützenswerte Personendaten sind, die unter Artikel 5 Buchstabe c Ziffer 5 DSG fallen. Unter diese spezifische Kategorie von besonders schützenswerten Daten fallen namentlich Angaben über die Eröffnung, die Durchführung und den Abschluss von Verfolgungen. Im Zeitpunkt der optischen Erfassung ist noch kein Verfahren eröffnet worden. Es besteht eine Vermutung wegen eines Verstosses nach Artikel 52 Absatz 1 Buchstabe g. Ob diese als «ausreichend» zu betrachten ist, kann im Vornherein nicht bestimmt werden.

Sollte die optische Erfassung zu einem Verwaltungsstrafverfahren führen, sind besonders schützenswerte Daten gemäss Artikel 5 Buchstabe c Ziffer 5 DSG betroffen, wozu es Folgendes auszuführen gilt:

Das Prinzip der Erkennbarkeit der Datenbeschaffung und der Erkennbarkeit ihres Zwecks (insbesondere wegen dem aus dem Prinzip von Treu und Glauben fliessenden Verbots der heimlichen Datenbeschaffung) durch die betroffenen Personen kann vorliegend in zulässiger Weise eingeschränkt werden. Artikel 18a Absatz 1 VStrR setzt bei Verwaltungsstrafverfahren voraus, dass die Behörde Daten für die betroffene Person erkennbar zu beschaffen hat, sofern das Verfahren dadurch nicht gefährdet wird. In denjenigen Fällen, in denen vermutungsweise Störsender in Fahrzeugen eingesetzt werden, würde alles durch eine vorgängige Information gefährdet und so könnten beispielsweise die Störsender beiseitegeschafft werden.

Die geplanten Massnahmen und Datenbearbeitungsschritte sind verhältnismässig. Es handelt sich um geeignete und erforderliche Massnahmen, um das Vorhandensein von Störungen in Fahrzeugen festzustellen und gegebenenfalls die für die Störungen verantwortlichen Personen zu ermitteln. Es ist nicht ersichtlich, inwiefern eine mildere Massnahme vorgesehen werden kann, um die Ursachen von Störfällen im Verkehr effektiv festzustellen und gegebenenfalls verfolgen zu können. Auch die Zweck-Mittel-Relation bleibt gewahrt: Die von Fahrzeugen ausgehenden Störungen können sicherheitsrelevante Frequenzen (z. B. Satellitennavigation) effektiv und nachhaltig stören und die Sicherheitsdienste (v. a. die Rettungsflugwacht) bei der Ausübung ihrer wichtigen Tätigkeit behindern.

Die Risikovorprüfung der Datenschutz-Folgenabklärung hat gezeigt, dass der Umfang der Datenverarbeitung nicht über das übliche Mass hinausgeht. Gestützt auf Artikel 26 Absatz 1 wird das Frequenzspektrum jeweils an einem geeigneten Ort kontrolliert. Im Rahmen dieser Aufsichtstätigkeit werden bei den Messungen nur die Kontrollschilder von jenen Fahrzeugen aufgenommen, bei denen ein störendes Signal (unabsichtliche und absichtliche Störungen) festgestellt wird. Es ist daher davon auszugehen, dass die Anzahl der von der automatisiert optischen Erfassung betroffenen Personen gering und

⁶¹ SR 313.0

die Bearbeitungsdauer relativ kurz ist. Die Überwachung erfolgt nicht permanent, sondern nur stichprobenartig. Die wenigen zu beschaffenden Messstellen sind deshalb auch nicht fest installiert.

Die Daten werden je nach zu beschaffendem System im System selbst oder in einem unabhängigen Rechner gespeichert.

Bei einer unabsichtlichen Störung werden die Daten der optisch erfassten Fahrzeuge nach der nachgelagerten Analyse umgehend ausgesondert und gelöscht. Eine geringe Fehlerquote bei der automatischen Auswertung der Störung des Frequenzspektrums ist nicht auszuschliessen. Folglich werden nicht verwertbare oder nicht mit dem Ereignis in Verbindung stehenden optischen Erfassungen («falsche positive Ergebnisse») sowie unbeteiligte Fahrzeuge durch die Fachpersonen ausgesondert und gelöscht.

Bei einer absichtlichen Störung sollen die Daten betreffend die automatisiert optisch erfassten Fahrzeuge bei der Vermutung auf das Mitführen eines Störsenders höchstens bis Abschluss des Verfahrens als Beweismittel abgespeichert bleiben. Sie dienen der Beweissicherung, um Störungen im Frequenzspektrum mit einem Verstoss gegen das FMG in Verbindung bringen zu können. Die durch die automatisiert optische Erfassung erhaltenen Daten sollen unverzüglich ausgesondert und gelöscht werden, sobald und falls sie nicht als Beweismittel dienen.

Auch wenn Personendaten bei den Messungen erhoben werden, handelt es nicht um ein Profiling im Sinne des Artikel 5 Buchstabe f DSGVO, da diese nicht verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, so wie es bei der automatischen Fahrzeugfahndung und Verkehrsüberwachung vorgesehen ist.

Das beabsichtige System lässt zudem keine automatisierte Einzelentscheidung zu; ein allfälliges Verfahren wird von den Mitarbeitenden des BAKOM eröffnet und von diesen bis zum Verfahrensabschluss durchgeführt.

Das BAKOM wird zudem über organisatorische und technische Massnahmen die Datensicherheit der Messapparaturen und der abgespeicherten Daten nach Artikel 13a Absatz 2 (vgl. Art. 8 DSGVO) gewährleisten sowie die entsprechende Bearbeitungstätigkeit in dem Verzeichnis festhalten, welches dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) abzuliefern ist (vgl. Art. 12 DSGVO).

Der Bundesrat soll die Einzelheiten hinsichtlich des zu beschaffenden Systems, den entsprechenden Anonymisierungsvoraussetzungen sowie der Aufbewahrungsdauer der Daten auf Verordnungsstufe regeln können. Dabei handelt es sich insbesondere um technische Ausführungen, welche bei Bedarf periodisch angepasst werden müssen. Eine Delegation an den Bundesrat ist deshalb angezeigt.

Abs. 4

Um wiederkehrende Störsignale im Mobilfunkbereich zeitlich und örtlich lokalisieren und einer spezifischen Fernmeldeanlage zuweisen zu können, ist es zwingend erforderlich, dass das BAKOM von den Anbieterinnen, Eigentümerinnen oder Betreiberinnen Informationen über die Entwicklung der Strahlungsdiagramme über einen bestimmten Zeitraum oder zu einem bestimmten Zeitpunkt (insbesondere zu den Abstrah-

lungseigenschaften und den Abstrahlungseinstellungen der betroffenen Anlage) gemäss Absatz 1 anfordern kann. Der Bundesrat soll die Einzelheiten in Bezug auf diese Informationen und den massgeblichen Zeitraum festlegen können.

Art. 35b Zugang zum Gebäudeeinführungspunkt und Mitbenutzung gebäudeinterner Anlagen

Mit Absatz 6 wird dem BAKOM neu die Kompetenz erteilt, Vorgaben für die Installation von Leitungen in Liegenschaften zu erlassen, soweit dies für die Gewährleistung eines sicheren, störungsfreien und diskriminierungsfreien Zugangs zu öffentlichen Fernmeldediensten erforderlich und zumutbar ist. In einem dynamischen Umfeld mit raschem technologischem Fortschritt ist es nicht möglich, den gesamten Regelungsbedarf vorab zu identifizieren.

Hinsichtlich des diskriminierungsfreien Zugangs hat das BAKOM im Frühjahr 2024 eine Branchenbefragung durchgeführt. Diese zeigte, dass es beim Ausbau der Glasfasernetze teilweise dazu kommt, dass Liegenschaften durch bauliche Massnahmen so erschlossen werden, dass es anderen Anbieterinnen verunmöglicht wird, die Liegenschaft ebenfalls zu erschliessen oder die gebäudeinterne Verkabelung mitzubeneutzen. Diese baulichen Hindernisse sind problematisch für den (Infrastruktur-)Wettbewerb. Nebst dem Verhindern von weiteren Anschlüssen durch Konkurrenten, können bauliche Hindernisse auch dazu führen, dass eine Zweiterschliessung nur mit höheren Kosten oder Verzögerung erfolgen kann. Beides führt zu Nachteilen im Wettbewerb und kann durch entsprechende Vorgaben adressiert werden. Auf technischer Ebene besteht mit den Richtlinien, die am runden Tisch der ComCom im Jahr 2012⁶² ausgearbeitet wurden, bereits ein Konsens der Branche, welcher mehrheitlich eingehalten wird. Die Möglichkeit, dass das BAKOM diese Richtlinien rechtlich verbindlich machen kann, schafft diesbezüglich zusätzliche Sicherheit.

In Bezug auf Störungen bieten sich Vorschriften an, die mit zumutbarem Aufwand dazu führen, dass konforme militärische Anwendungen und private Internetverbindungen störungsfrei nebeneinander betrieben werden können. Dies kann beispielsweise dadurch erreicht werden, dass gebäudeinterne Anlagen mit genügender Schirmung erstellt werden. Ob Regelungen für bestehende Anlagen in Frage kommen, hängt entscheidend vom damit verbundenen Aufwand ab. Dieser muss für Liegenschaftseigentümer zumutbar sein.

Art. 46 Persönlichkeitsschutz

In den bereits bestehenden Artikel soll ein zusätzlicher Absatz eingefügt werden. Gestützt auf diese Bestimmung (vgl. Abs. 1) hat der Bundesrat im geltenden Recht Ausführungsbestimmungen zur Identifikation des anrufenden Anschlusses auf Verordnungsstufe erlassen. Er hat insbesondere festgelegt, dass die Teilnehmerinnen und Teilnehmer bei einem Anruf grundsätzlich die Möglichkeit haben müssen, ihre Telefonnummer unterdrücken zu lassen, so dass sie den Angerufenen nicht bekanntgegeben beziehungsweise auf deren Endgerät nicht angezeigt wird (vgl. Art. 84 Abs. 1 FDV). Die Anrufenden können so eine unerwünschte Identifikation durch die Anzeige ihrer Telefonnummer verhindern. Er hat ebenfalls vorgesehen, wann eine Telefonnummer den Angerufenen ausnahmsweise dennoch angezeigt werden soll, obwohl die Anrufenden sie diesen nicht bekanntgeben möchten. Diese GegenAusnahmen, beschrän-

⁶² BAKOM (2012)

ken sich einerseits auf die Standortidentifikation, welche die Anbieterinnen von Fernmeldediensten bei der Sicherstellung des Zugangs zu den Notdiensten nach Artikel 20 und im Rahmen der Sicherheitskommunikation nach Artikel 47 sicherstellen müssen, sowie andererseits für die Anrufe auf den Transkriptionsdienst für Hörbehinderte (vgl. Art. 84 Abs. 3 FDV).

In Absatz 2 sollen neu die Voraussetzungen aufgeführt werden, unter denen der Bundesrat festlegen kann, wann die Anbieterinnen von Fernmeldediensten die Anzeige der anrufenden Anschlüsse auch garantieren und somit eine bestehende Rufnummernunterdrückung deaktivieren müssen. Der Bundesrat berücksichtigt bei dieser Festlegung die Interessen der Bevölkerung, der Angerufenen und der Anbieterinnen sowie die technische Entwicklung und die internationale Harmonisierung. Der Bundesrat kann so beispielweise für Festnetzanschlüsse der Blaulichtorganisationen wie beispielsweise der Polizei, die Garantie der Anzeige der Telefonnummer der anrufenden Personen vorsehen, damit diese aus ermittlungstaktischen Gründen in zeitkritischen Szenarien wie Drohanrufen (Amokläufe, Bombendrohungen) zumindest eine Telefonnummer angezeigt erhalten. Derartige Anrufe oder Hinweise gehen nicht nur über den Polizeinotruf (117) ein, bei der die Anzeige der Telefonnummer des anrufenden Anschlusses bereits heute sichergestellt werden muss. Oftmals erfolgen entsprechende Anrufe auch über die geografischen Festnetznummer der Polizei, bei denen die Anzeige derzeit weder sichergestellt werden muss und noch darf. Dem Bundesrat soll die Möglichkeit haben, die Aufhebung der Rufnummernunterdrückung auch auf solche Anschlüsse ausdehnen zu können und dies auch ohne ausdrückliche Zustimmung der anrufenden Teilnehmerinnen und Teilnehmer.

Art. 46a Kinder- und Jugendschutz

Durch Annahme der Motion Gugger (20.3374) wird der Bundesrat beauftragt, der Bundesversammlung die gesetzlichen Anpassungen vorzulegen, dass der Zugang zu legaler Pornographie für Personen unter 16 Jahren erschwert oder verunmöglicht wird. Hierzu sollen die Anbieterinnen von Fernmeldediensten verpflichtet werden, die Erziehungsberechtigten auf die technischen Möglichkeiten bei Endgeräten und Angeboten hinzuweisen sowie ihnen Tools und Apps anzubieten, mit denen Jugendliche wirksam vor pornografischen Inhalten geschützt werden können.

Die Anbieterinnen von Fernmeldediensten müssen deshalb zukünftig die Erziehungsberechtigten zum Jugendschutz individuell beraten. Sie müssen ihnen auch Mittel zur Verfügung stellen, die entsprechend dem Stand des technisch Möglichen wirksam den Jugendschutz gewährleisten können.

Die Absätze 2 und 3 werden materiell nicht geändert. Es erfolgt lediglich eine redaktionelle Anpassung, bei welcher der Begriff «Bundesamt für Polizei» durch «fedpol» ersetzt wird.

Art. 48a Resilienz der Fernmeldeinfrastrukturen und Schutz vor Cyberbedrohungen

Die erweiterten Massnahmen in Artikel 48a sind Teil eines gesamtheitlichen Ansatzes zur Verbesserung der Sicherheit und der Resilienz der Fernmeldeinfrastrukturen in der Schweiz. Nebst bereits teilweise bestehenden Pflichten für die Anbieterinnen von Fernmeldediensten soll auch die Zusammenarbeit mit anerkannten Stellen im Bereich der Cybersicherheit ermöglicht werden und der Informationsaustausch mit dem BAKOM im

Bereich der Cybersicherheit geklärt werden. Dazu soll auch das BAKOM mit Aufgaben zur Sicherstellung der Resilienz beitragen. Letztlich sind diese Massnahmen gemeinsam mit den Vorgaben in Artikel 48b zur Sicherheit der Fernmeldeinfrastruktur an sich und den Eingriffsmöglichkeiten des Bundesrates in Artikel 48c als globalen Sicherheitsbeitrag zu betrachten. Sie sollen den neu im Zweckartikel aufgenommene Schutz vor Cyberbedrohungen und die Gewährleistung der Sicherheit und der Resilienz von Fernmeldeinfrastrukturen konkretisieren (vgl. Art. 1 Abs. 2 Bst. b und f).

Abs. 1

Die Schweiz sieht sich aufgrund der aktuellen geopolitischen Lage und der stetigen Zunahme von Cyberangriffen auf die Fernmeldeinfrastrukturen einer grossen Bedrohung ausgesetzt. So hat der Bundesrat⁶³ festgehalten, dass die Bedrohung durch Cyberangriffe seit Jahren anhaltend hoch sei und die Abhängigkeit der Wirtschaft und Gesellschaft von funktionierenden Informations- und Kommunikationstechnologie-Umgebungen (IKT) weiter ansteige. Die Cybersicherheit ist auf verschiedenen Ebenen wichtig geworden. So auch in der Sicherheitspolitik, als Voraussetzung für die Digitalisierung, im Bereich des Datenschutzes und nicht zuletzt ist sie unabdingbar für den Wirtschafts- und Forschungsstandort Schweiz. Das BACS stellt vermehrt Cyberangriffen auf Ziele in der Schweiz fest, darunter Angriffe auf die Betreiber von kritischen Infrastrukturen, die durch Fernmeldeinfrastrukturen in der Schweiz ermöglicht werden.

Es ist deshalb von zentraler Bedeutung, dass die Schweiz die Resilienz ihrer Fernmeldeinfrastrukturen stärkt und die Anbieterinnen die dazu notwendigen technischen, operativen und administrativen Massnahmen ergreifen. Diese Tendenz lässt sich auch in der Politik beobachten; in diversen Vorstössen werden ähnliche Forderungen gestellt. Als Beispiele seien hier das Postulat Z`Graggen (22.4411) «*Strategie Digitale Souveränität der Schweiz*», die Motion Dittli (23.3002) «*Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz*» sowie die Motionen Juillard (24.3209) und Chappuis (24.3363) «*Für eine souveräne digitale Infrastruktur in der Schweiz im Zeitalter der künstlichen Intelligenz*» erwähnt.

Die Resilienz der Fernmeldeinfrastrukturen in der Schweiz beinhaltet, dass die Stabilität und die Sicherheit der Fernmeldeinfrastrukturen gewährleistet werden muss und zu deren Schutz regulatorische Massnahmen ergriffen werden können. Sie umfasst auch die Fähigkeit der Netze, einzelne Dienste weiter zu betreiben, wenn andere Dienste ausgefallen sind, sowie die Fähigkeit, Dienste unabhängig von der Verfügbarkeit ausländischer Dienste weiter zu betreiben. In diesem Zusammenhang ist die Cybersicherheit von Fernmeldeinfrastrukturen und Fernmeldediensten eine grosse Herausforderung für die Schweiz, da sie in diesem Bereich aufgrund der massiven Nutzung von Informationstechnologien besonders anfällig ist⁶⁴.

Artikel 48a Absatz 1 sieht bereits in seiner geltenden Fassung eine Pflicht für Anbieterinnen von Fernmeldediensten zur Bekämpfung der unbefugten Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen vor. Gemäss der Botschaft zur letzten Revision des FMG⁶⁵ hat diese Bestimmung die Bekämpfung von Cyberangriffen (z.B. Verteilung von Schadsoftware, Beeinträchtigung von Web-Diensten durch DDoS-Attacken) zum Ziel. Im Lichte des nun erweiterten Zweckartikels hinsichtlich des

⁶³ Bundesrat (2023a)

⁶⁴ Schwaab (2023)

⁶⁵ BBl 2017 6659

Schutzes vor Cyberbedrohungen und der Stärkung der Resilienz der Fernmeldeinfrastrukturen sollen diese Grundsätze auch klar als Aufgabe für die Anbieterinnen verankert werden. Dazu haben sie technische, operative und administrative Massnahmen zu ergreifen, um die unbefugte Manipulation von Fernmeldeinfrastrukturen durch fernmeldetechnische Übertragungen zu bekämpfen. Sie sind zu diesem Zweck weiterhin berechtigt, Verbindungen umzuleiten oder zu verhindern und Informationen zu unterdrücken.

Abs. 2

Um die erweiterten Massnahmen nach Artikeln 48a und 48b wirksam umsetzen zu können, sollen nicht nur die Anbieterinnen einen Beitrag leisten. Vielmehr soll auch das BAKOM in diesem Bereich neue Aufgaben wahrnehmen, damit die mit diesen Massnahmen angestrebten Ziele vollumfänglich erreicht werden können. So soll es künftig Risikofaktoren überwachen, ermitteln und bewerten, welche die Resilienz der Fernmeldeinfrastrukturen gefährden oder den Schutz vor Cyberbedrohungen beeinträchtigen können. Mit dieser Tätigkeit soll es insbesondere das Vorliegen eines Sicherheitsrisikos für die Fernmeldeinfrastrukturen nach Artikel 48b evaluieren. Es ist anzumerken, dass das BAKOM zwar auf der Grundlage der ihm vorliegenden technischen, operativen und administrativen Daten oder Informationen für die ordnungsgemässe Umsetzung der Artikeln 48a und 48b zuständig ist (vgl. Abs. 3), die Anwendung von Artikel 48c hingegen dem Bundesrat vorbehalten ist. Für eine entsprechende Massnahme hätte er sich auf die ihm von den zuständigen Behörden und Fachstellen des Bundes vorgelegten geopolitischen Einschätzungen zu stützen.

Abs. 3

Im Rahmen der in Absatz 2 vorgesehenen Aufgaben des BAKOM kann die Auskunft zu bestimmten Daten und Informationen von Anbieterinnen von Fernmeldediensten für einen effizienten Schutz vor Cyberbedrohungen erforderlich sein. Der Zugang zu diesen Daten trägt wesentlich dazu bei, die Sicherheitsrisiken in Zusammenhang mit den Fernmeldeinfrastrukturen und die Herkunft und sicherheitsrelevanten Folgen gezielter Bedrohungen wie Cyberangriffe vom Typ DDoS, *Phishing* oder die Verbreitung von *Malware* zu erkennen und zu identifizieren. In solchen Fällen kann sich die in den Netzwerken zunehmend verwendete biometrische Identifikation als entscheidend erweisen, um eine Handlung einer spezifischen Person zuzuordnen oder die unzulässige Nutzung von fernmelderechtlich erfassten Ressourcen feststellen zu können, die auf eine cyberkriminelle Handlung hinweisen kann (vgl. Art. 48d Abs. 1). Auch wenn Anbieterinnen von Fernmeldediensten zur Herausgabe von Verkehrsdaten verpflichtet sind, so dürfen und können sie in keinem Fall den Inhalt von Telekommunikationsverbindungen herausgeben oder davon Kenntnis erlangen. Diese Inhalte sind und bleiben auch in Zukunft streng durch das Fernmeldegeheimnis geschützt (vgl. Art. 13 Abs. 1 BV, 321^{ter} StGB und 43 FMG).

Abs. 4

Absatz 4 entspricht grundsätzlich Absatz 2 der geltenden Fassung und soll dabei noch mit einer Rechtssetzungsdelegation des Bundesrates hinsichtlich der Präzisierung der Massnahmen nach Absatz 1 ergänzt werden. Bereits gemäss der geltenden Fassung dieses Absatzes, kann der Bundesrat für die Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten Bestimmungen insbesondere betreffend die Verfügbarkeit, den Betrieb, Sicherstellung von redundanten Infrastrukturen, Meldung

von Störungen, Nachvollziehbarkeit von Vorgängen und die Umleitung oder Verhinderung von Verbindungen sowie Unterdrückung von Informationen nach Absatz 1 erlassen. Aufgrund dieser Kompetenzdelegation hat der Bundesrat bereits die Artikel 96a ff. über die unbefugte Manipulation von Fernmeldeanlagen sowie die Artikel 96f ff. über Sicherheit von Netzen und Diensten der Mobilfunkkonzessionärinnen festgelegt. Er beabsichtigt im Übrigen in der Teilrevision der Verordnungen im Fernmeldebereich «*Erhöhung der Netzsicherheit und Schutz vor Cyberbedrohungen*», welche parallel zu dieser FMG-Revision in die öffentliche Vernehmlassung geschickt wird, Neuregelungen einzuführen, die strengere Sicherheitsanforderungen für die Anschaffung und den Betrieb von Fernmeldeanlagen und Software bezwecken. Darüber hinaus soll insbesondere eine Verpflichtung für Mobilfunkkonzessionärinnen und «*Full Mobile Virtual Network Operator*» (*Full MVNO*) festgelegt werden, regelmässig die Konformität ihres Kernnetzes mit den verschärften Sicherheitsanforderungen zu überprüfen.

Zusammenfassend ist der Bundesrat im Rahmen der in Absatz 4 vorgesehenen Kompetenzdelegation befugt, auf Verordnungsstufe die erforderlichen Massnahmen über die Sicherheit von Informationen sowie von Fernmeldeinfrastrukturen und -diensten zu ergreifen, die zum Schutz vor Gefahren, zur Vermeidung von Schäden und zur Minimierung von Risiken beitragen.

In diesem Zusammenhang bezieht sich der allgemeine Begriff der Fernmeldeinfrastruktur auf die Gesamtheit der Fernmeldeanlagen respektive Hardware- und Softwaresysteme der Telekommunikation. Unter den Begriff fallen alle Produkte, Bestandteile von Produkten und Hardware- oder Softwarekomponenten (*Computercode*), die zur Integration in die Fernmeldeinfrastruktur bestimmt sind und deren vorgesehene oder vernünftigerweise vorhersehbare Verwendung dem Angebot von Fernmeldediensten dient. Insbesondere umfasst der Begriff sämtliche Hardware- (Server, Übertragungs- und Speicherungseinrichtungen, Netzausrüstungen) und Softwarekomponenten (Betriebssysteme, Virtualisierungstools, Lösung für die Verwaltung, Pflege und Überwachung von Inhalten), einschliesslich elektrischer, elektronischer oder IT-Geräte, die an der Bereitstellung von technischen Verarbeitungs-, Verwaltungs-, Speicherungs-, Übertragungs- oder Datenzugangsdiensten für Dritte beteiligt sind.

Der Begriff der Fernmeldeinfrastruktur ist folglich weiter gefasst als jener der Fernmeldeanlage nach Artikel 3 Buchstabe d. Er umfasst einerseits Anlagen, elektrische Geräte einschliesslich deren Software, Betriebssysteme sowie andere Lösungen für das digitale Informationsmanagement wie andererseits auch die Kabelkanalisationen.

Art. 48b Sicherheit von Fernmeldeinfrastrukturen

Der Bericht des Bundesrates in Erfüllung des Postulates Pult (20.3984) «*Digitale Infrastruktur. Geopolitische Risiken minimieren*»⁶⁶ hat gezeigt, dass trotz der bereits getroffenen Massnahmen weiterhin grosse Cyberbedrohungen bestehen. Die Schweiz ist Sicherheitsrisiken ausgesetzt, da viele unserer wirtschaftlichen, gesellschaftlichen oder politischen Prozesse durch digitale Netzwerke und Systeme gesteuert werden. Diese können Sicherheitslücken aufweisen oder Ziel von Cyberangriffen sein. Zudem können über die Fernmeldeinfrastruktur andere kritische Infrastrukturen gehackt oder sabotiert werden. Nach Ansicht des Bundesrates ist es daher notwendig, den Kampf gegen diese Cyberbedrohungen zu verstärken, indem Massnahmen zur Diversifizierung der Hersteller von als risikobehaftet geltenden Ausrüstungen für Fernmeldeinfrastrukturen ergriffen werden. Diese Massnahmen sind im neuen Artikel 48b vorgesehen und sollen

⁶⁶ Bundesrat (2023a)

konkret auch dem im Zweckartikel aufgenommenen Ziel zur Gewährleistung der Sicherheit und der Resilienz von Fernmeldeinfrastrukturen beitragen (vgl. Art. 1 Abs. 2 Bst. f)

Das FMG regelt das Angebot von Fernmeldediensten, indem es diese dem freien Wettbewerb unterwirft (vgl. Art. 1 Abs. 1 und 2 Bst. c). Dieser freie Wettbewerb gilt im Übrigen auch bei den Infrastrukturen. So sind die Anbieterinnen von Fernmeldediensten nach dem FMG frei in der Wahl ihrer Gerätehersteller sowie Anlagen und weiteren Infrastrukturen, die sie in ihrer Fernmeldeinfrastruktur erwerben, in Betrieb nehmen und betreiben wollen. Eine Einschränkung der freien Wahl der Anbieterinnen im Bereich der Fernmeldeinfrastruktur bedarf deshalb einer gesetzlichen Grundlage (vgl. Art. 36 Abs. 1 BV), da diese in ihre Wirtschaftsfreiheit (vgl. Art. 27 BV) und die Eigentumsgarantie (vgl. Art. 26 BV) eingreift. Mit Artikel 48b wird diese formelle gesetzliche Grundlage geschaffen, die die Einschränkung der freien Wahl der Anbieterin bezüglich ihrer Infrastruktur erlaubt.

Die Verminderung von Cyberbedrohungen, Schwachstellen und anderen Sicherheitslücken, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten im Fernmeldeverkehr beeinträchtigen können, erfordert die Sicherung der Produkte und Hardware- oder Softwarekomponenten, die Bestandteil der Fernmeldeinfrastruktur sind. Wenn es sich bei diesen Produkten und anderen Komponenten um Fernmeldeanlagen nach Artikel 3 Buchstabe d handelt, müssen sie die Cybersicherheitsanforderungen erfüllen und die Konformitätsbewertungsverfahren durchlaufen, die in der FAV und in der VFAV vorgesehen sind, bevor sie in der Schweiz angeboten, in Verkehr gebracht oder betrieben werden dürfen. In diesen Verordnungen können somit Cybersicherheitsanforderungen für diejenigen Anlagen festgelegt werden, die zur Integration in der Fernmeldeinfrastruktur bestimmt sind. Aufgrund der mit Artikel 48a Absatz 4 vorgesehenen Kompetenzdelegation im Bereich der Infrastrukturen kann der Bundesrat diese Regelung der FAV und VFAV auf Infrastrukturen anwenden bzw. ausweiten, die keine Fernmeldeanlagen im engeren Sinne darstellen, etwa Software, elektrische Geräte oder Betriebssysteme und andere Systeme zur Verwaltung der Cybersicherheit.

Durch die Tatsache, dass die Fernmeldeinfrastruktur nach Artikel 48a Absatz 4 allgemein alle Produkte mit digitalen Elementen im Sinne der Verordnung (EU) 2024/2847⁶⁷ umfasst, kann dem Umstand Rechnung getragen werden, dass die Cybersicherheitsanforderungen neu weitgehend horizontal und unabhängig von den betroffenen Branchen ausgestaltet sind. Auf dieser Grundlage kann sich die Schweiz auf die technischen Normen der europäischen Komitees für Normung beziehen und in Anbetracht des MRA Schweiz–EU⁶⁸, das Handelshemmnisse zwischen der Schweiz und der EU verhindert, ihre Regulierung mit dem europäischen Recht und den Zertifizierungssystemen im Bereich der Cybersicherheit, insbesondere für die von der EU-Agentur für Cybersicherheit (*European Network and Information Security Agency*, ENISA) vorgesehenen 5G-Netze, harmonisieren.

Abs. 1

In Absatz 1 wird das Grundprinzip der Sicherheit durch Technikgestaltung und Voreinstellungen (*Secured by Design and by Default*) im Gesetz verankert, das im Bereich des Erwerbs, der Inbetriebnahme und des Betriebs der Fernmeldeinfrastrukturen massgeblich ist. Es bedeutet, dass nur Anlagen, Geräte, Produkte und andere Hardware-

⁶⁷ Siehe Fussnote 27.

⁶⁸ SR 0.946.526.81

oder Softwarekomponenten, die von Anfang an sicher konzipiert, hergestellt und konfiguriert wurden, in Fernmeldenetze integriert werden dürfen. Dadurch ist es möglich, das Risiko von Sicherheitslücken ohne vorherige Intervention der Anbieterinnen zu verringern und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen. Das Prinzip lässt sich aus der allgemeinen Sicherheitspflicht (vgl. Art. 48a) und aus dem Fernmeldegeheimnis (vgl. Art. 43, Art. 13 Abs. 1 BV und Art. 321^{ter} StGB) ableiten. In Absatz 1 wird die Tragweite des Prinzips festgelegt. Mit der Präzisierung, dass die Sicherheitseinstellungen nicht nur aktiviert, sondern standardmässig konfiguriert sein müssen, wird unterstrichen, dass diese Einstellungen nicht nur einfach mit den Werkseinstellungen aktiviert, sondern auch unter Beachtung der besten Praktiken (*Best Practices*) im Bereich der Sicherheit korrekt konfiguriert sein müssen. Im Übrigen ist es wesentlich, dass diese Einstellungen regelmässig gepflegt und auf dem neuesten Stand gehalten werden. Die hardware- und softwarebasierten Massnahmen und Technologien, die die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen nach Absatz 1 schützen, müssen sich möglichst an den internationalen Normen und Standards in diesem Bereich orientieren.

Abs. 2

Absatz 2 verpflichtet die Anbieterinnen von Fernmeldediensten zu einer Mehrlieferantenstrategie. So müssen sie in ihren Netzen Bestandteile von Fernmeldeinfrastrukturen von verschiedenen Herstellern erwerben, in Betrieb zu nehmen und betreiben. Jede Anbieterin muss für ihr eigenes Fernmeldenetz eine solche Strategie umsetzen. Sie verstärkt die Sicherheit, indem für die Erbringung von Fernmeldediensten eine Vielzahl verschiedener Geräte, Produkte und anderer Hardware- oder Softwarekomponenten verwendet und so eine gleichförmige technologische Umgebung, die Cyberangriffe begünstigt, verhindert wird. Ziel ist auch, das Risiko einer grossen Abhängigkeit von einem Hersteller zu begrenzen und mehr Flexibilität und Resilienz hinsichtlich der Lieferketten von Fernmeldeinfrastrukturen sicherzustellen. Dies auch aufgrund der Tatsache, dass es in unserem Land keine wesentlichen Gerätehersteller gibt. Unter Hersteller ist dabei jede natürliche oder juristische Person, die eine Fernmeldeanlage herstellt beziehungsweise entwickeln oder herstellen lässt und diese Anlage unter ihrem Namen oder ihrer Handelsmarke in Verkehr bringt (vgl. in diesem Sinne Art. 2 Bst. I FAV).

Die meisten Anbieterinnen, vor allem im Mobilfunkbereich, verfolgen bereits aus eigenem Antrieb eine Mehrlieferantenstrategie. Die Verpflichtung zu einer Mehrlieferantenstrategie im Sinne von Absatz 2 betrifft ausschliesslich die kritischen Bestandteile der Fernmeldeinfrastruktur einer Anbieterin, nämlich die Bestandteile deren Störung oder Fehlfunktion die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der übertragenen Informationen beeinflussen und dadurch zu einem Ausfall oder einer erheblichen Beeinträchtigung des Betriebs von Fernmeldeinfrastrukturen führen oder die öffentliche Sicherheit gefährden kann. Grundsätzlich sollte der Bundesrat nur dann tätig werden und von seiner Kompetenz zur Festlegung der Kategorien, Teile, Anteile oder Mindestprozensätze von betroffenen kritischen Infrastrukturen Gebrauch machen, wenn er einen besonderen Mangel an Vielfalt in wesentlichen Teilen der Fernmeldesysteme feststellt, etwa Elementen des Mobilfunk-Kernnetzes (*Core Network*) oder von Funkzugangnetzen (*Radio Access Network, RAN*).

In jedem Fall muss mindestens einer der von der Anbieterin gewählten Hersteller in einem Staat domiziliert sein, dessen Gesetzgebung einen angemessenen Datenschutz

gewährleistet (vgl. Art. 8 und 16 DSGVO sowie Anhang 1 der Verordnung vom 31. August 2022⁶⁹ über den Datenschutz, DSV). Von diesen Herstellern wird angenommen, dass sie die Anforderungen der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen für ihre Produkte, Anlagen und anderen Geräte, die für die Fernmeldeinfrastruktur bestimmt sind, in Übereinstimmung mit den Verpflichtungen ihres Sitzstaats zum Schutz der Privatsphäre erfüllen. Dies schränkt das Risiko erheblich ein, dass ein solcher Hersteller unter Artikel 48c fällt, da er als problematisch für die Sicherheit unseres Landes gelten würde oder sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befände, der ein geopolitisches Risiko für das Land darstellt. Als Herstellerin im Sinne dieser Bestimmung gilt die Muttergesellschaft beziehungsweise die kontrollierende juristische oder natürliche Person, unabhängig von verwendeten Markennamen oder Tochtergesellschaften.

Abs. 3

Angesichts der Bedeutung der Fernmeldeinfrastrukturen für das Funktionieren unseres Landes und der Cyberbedrohungen, denen sie ausgesetzt sind, muss die Regulierung in diesem Bereich nach dem Vorbild der «5G-Toolbox» der EU⁷⁰ und der meisten nationalen Gesetzgebungen der EU-Mitgliedstaaten verstärkt werden. Gestützt auf Absatz 3 kann das BAKOM die Anbieterinnen von Fernmeldediensten deshalb verpflichten, kritische Bestandteile von Infrastrukturen nicht in Betrieb zu nehmen oder aus ihren Netzen zu entfernen, bei denen ein begründeter Verdacht besteht, dass sie ein besonders schwerwiegendes Sicherheitsrisiko für die Fernmeldenetze darstellen. Das besondere Sicherheitsrisiko bezieht sich auf die kritischen Bestandteile oder auf die integrale und vertrauliche Übertragung der Informationen sowie auf ihre Verfügbarkeit. Die Pflicht betrifft vor allem die wesentlichen Teile der Fernmeldenetze wie Elemente des Mobilfunk-Kernnetzes (*Core Network*) oder von Funkzugangnetzen (RAN). Das besondere Sicherheitsrisiko für die Fernmeldeinfrastruktur oder für die Übertragung der Informationen bezieht sich auf ein Cybersicherheitsrisiko, bei dem aufgrund seiner technischen Merkmale davon auszugehen ist, dass es mit hoher Wahrscheinlichkeit zu einem Vorfall führen wird, der schwerwiegende Auswirkungen haben und erhebliche materielle oder immaterielle Verluste oder Störungen verursachen könnte.

Das BAKOM muss in einer Liste die kritischen Bestandteile von Infrastrukturen konkret festlegen, deren Einsatz und Betrieb untersagt würden, und diese veröffentlichen. Da sich Technologien, Infrastrukturen und Cyberbedrohungen ständig weiterentwickeln, müsste die Liste laufend angepasst und auf dem neuesten Stand gehalten werden. Daher soll die Liste grundsätzlich als Anhang zu einer Verordnung ausgestaltet werden, die ein periodisches Nachführen zulassen würde. Zur Feststellung eines solchen Sicherheitsrisikos stützt sich das BAKOM auf die Informationen und Daten, die ihm von den Anbietern von Fernmeldediensten (vgl. Art. 48a Abs. 3) und von den Herstellern von Fernmeldeinfrastrukturen (vgl. Art. 59 Abs. 1) übermittelt werden. Bei Bedarf könnte das BAKOM hierzu gestützt auf Artikel 48d Absatz 2 auch das BACS, das Staatssekretariat für Wirtschaft (SECO), das SEPOS, den Nachrichtendienst des Bundes (NDB) oder andere zuständige Stellen des Eidgenössischen Departementes für auswärtige Angelegenheiten (EDA), des Eidgenössischen Departementes für Verteidigung, Bevölkerungsschutz und Sport (VBS) oder des UVEK konsultieren. Weiter kann sich das BAKOM auf Forschungen und Studien von ausländischen Behörden oder anerkannten privaten und öffentlichen Stellen im Sinne von Artikel 29 abstützen, die Bedrohungen oder Sicherheitsvorfälle erkennen, um eine Gefährdung der Sicherheit oder

⁶⁹ SR 235.11

⁷⁰ EU (2020)

der Resilienz, die die Fernmeldeinfrastrukturen betreffen oder betreffen könnten, festzustellen und zu beurteilen.

Unter den weit gefassten Begriff der Fernmeldeinfrastruktur fallen grundsätzlich alle Bestandteile eines Netzes sowie elektrische oder elektronische Geräte, Produkte oder Hardware- oder Softwarekomponenten, die zum Funktionieren oder zur Sicherung eines Fernmeldenetzes beitragen (vgl. dazu auch die Erläuterungen zu Art. 48a). Grundsätzlich kann auch die Überwachungsinfrastruktur, welche den Anforderungen des BÜPF genügen muss, unter den Begriff der Fernmeldeinfrastruktur fallen. Dass dabei auch diese Überwachungsinfrastruktur sicher sein soll, ist dieser inhärent. Dennoch ist es zentral, dass die Anforderungen und Pflichten für die Anbieterinnen, die sich aus dem BÜPF ergeben, beachtet und sichergestellt sein müssen. Daher soll das BAKOM vor einer Verfügung über eine Entfernung oder Ausserbetriebnahme von kritischen Bestandteilen mit dem Dienst ÜPF vorgängig Rücksprache nehmen, sofern die betroffenen Bestandteile die Überwachungsinfrastruktur tangieren.

Art. 48c Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken

Abs. 1

In Anbetracht der Sicherheitsrisiken im Zusammenhang mit der starken Zunahme von Cyberangriffen und anderen Cyberbedrohungen ist es von zentraler Bedeutung, dass die Schweiz ihre Cyberresilienz durch die in den Artikeln 48a und 48b vorgesehenen technischen und operativen Sicherheitsmassnahmen für ihre digitalen Infrastrukturen stärkt. Diese allgemeinen Massnahmen sind durch geopolitische Mittel gemäss den Vorschlägen des Bundesrates in seinem Bericht in Erfüllung des Postulates Pult (20.3984)⁷¹ zu ergänzen. Dabei ist einem sich verschlechternden sicherheitspolitischen Umfeld der Schweiz, der zunehmenden Bedeutung von Spionage angesichts der anhaltenden globalen Konfrontationen, einer geschwächten europäischen Sicherheit, die gestärkt werden soll, und sich zuspitzenden Rivalitäten auf globaler Ebene Rechnung zu tragen⁷². Von einer Zuspitzung ist auszugehen, wenn sich sicherheitspolitische Risiken durch staatliche oder staatsnahe Akteure im Technologiebereich akut verschärfen, insbesondere durch Cyberangriffe, Sabotage, Erpressung, politischen oder wirtschaftlichen Druck mit Folgen für kritische Infrastrukturen.

Ähnlich wie es die «5G-Toolbox» der EU⁷³ vorsieht und von den meisten Mitgliedstaaten in ihrer Gesetzgebung konkretisiert wurde, ermöglicht Artikel 48c dem Bundesrat, bei einem die Schweiz bedrohenden sicherheits- oder geopolitischen Risiko durch Verordnung die notwendigen Massnahmen zu ergreifen. In erster Linie kann der Bundesrat den Anbieterinnen von Fernmeldediensten vorgängig den Erwerb 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 (vgl. Abs. 1). Der Begriff der Fernmeldeinfrastruktur umfasst grundsätzlich alle Bestandteile eines Netzes sowie elektrische oder elektronische Geräte, Produkte oder Hardware- oder Softwarekomponenten, die zum

⁷¹ Bundesrat (2023a)

⁷² Bundesrat (2025a)

⁷³ EU (2020)

Funktionieren eines Fernmeldenetzes beitragen (vgl. dazu auch die Erläuterungen zu Art. 48a).

Abs. 2

Artikel 48c ermöglicht dem Bundesrat, bei Bedarf zu handeln, um in einer Zeit geopolitischer Unsicherheit, welche die internationalen politischen und wirtschaftlichen Beziehungen stark prägt, die grundlegenden Interessen der Schweiz zu wahren. Gemäss Absatz 2 hat der Bundesrat bei der Beurteilung der geopolitischen Lage die innere und äussere Sicherheit sowie den Schutz des Werk-, Wirtschafts- und Finanzplatzes der Schweiz zu berücksichtigen. Im Rahmen der Interessenabwägung soll er mögliche Sanktionierungen (vgl. Bst. a), die wirtschaftlichen, technologischen und sicherheitsbezogenen Abhängigkeiten (vgl. Bst. b) und die globale sicherheitsrelevante Gefährdungslage anhand der Cyberangriffe, Sabotageakte oder sonstigen nachrichtendienstlichen Aktivitäten (vgl. Bst. c) miteinbeziehen. Es gilt dabei zu vermeiden, dass durch eine potenzielle Abhängigkeit von Lieferanten von kritischen Infrastrukturen, die Schweiz politisch unter Druck gesetzt werden könnte⁷⁴ oder die Schweiz im Gegenzug selbst von Sanktionen oder Embargos bedroht wäre, falls sie aufgrund der Nutzung bestimmter Infrastrukturen als Sicherheitslücke mitten in Europa betrachtet würde (vgl. Abs. 2 Bst. d). Vor diesem Hintergrund wäre der Bundesrat möglicherweise gezwungen, wichtige politische und wirtschaftliche Partner, mit denen die Schweiz eine enge Beziehung pflegt, zu bevorzugen und unter Berücksichtigung ihres auf Freiheit und Rechtsstaatlichkeit basierenden Wertesystems Entscheidungen zu treffen.

Der Bundesrat soll sich dabei auf die geopolitischen Einschätzungen stützen, die ihm von den zuständigen Behörden und Fachstellen des Bundes vorgelegt werden. Die Umsetzung von Artikel 48c erfordert angesichts der erheblichen aussen- und sicherheitspolitischen Implikationen eine gewisse Formalisierung der Koordinierung zwischen den betroffenen Behörden und Fachstellen.

Abs. 3

Über die vorsorglichen Massnahmen betreffend den Erwerb (vgl. Abs. 1) hinaus kann der Bundesrat die Anbieterinnen von Fernmeldediensten verpflichten, Bestandteile, die von geopolitisch problematischen Herstellerinnen stammen, aus ihrer Fernmeldeinfrastruktur zu entfernen. Eine solche Massnahme kann weitreichende Folgen für das Funktionieren der Netze und die operative Erbringung der Fernmeldedienste sowie wirtschaftliche und finanzielle Auswirkungen für die betroffenen Anbieterinnen haben. Es soll deshalb nur als letztes Mittel darauf zurückgegriffen werden. Dabei sind ausreichend lange Umsetzungsfristen vorzusehen, die den operativen Übergang der Netze sowie des Dienstangebots gewährleisten und die für die Amortisation und technologische Erneuerung der Fernmeldeinfrastrukturen benötigten Zeit berücksichtigen.

Das Verfahren für das Verbot muss vom Bundesrat in einer Verordnung näher festgelegt werden. Es muss so ausgestaltet sein, dass die von der Massnahme betroffenen Fernmeldediensteanbieterinnen und Herstellerinnen ihr Recht auf Anhörung geltend machen können. Wie unter Absatz 2 ausgeführt, würden Massnahmen nach dieser Bestimmung eine Formalisierung der Koordinierung zwischen den betroffenen Behörden

⁷⁴ Bundesrat (2023a)

und Fachstellen erfordern. Soweit die Sicherstellung der Überwachung des Fernmeldeverkehrs im Sinne des BÜPF durch eine Massnahme nach Absatz 3 betroffen sein könnte, wäre auch der Dienst ÜPF vorgängig zu konsultieren.

Das Bundesgesetz vom 13. Dezember 2002⁷⁵ über die Bundesversammlung (Parlamentsgesetz, ParlG) sieht besondere Regeln für Verordnungen vor, die der Bundesrat aufgrund einer gesetzlichen Kompetenz zur Krisenbewältigung erlässt. Diese Rechtsgrundlagen sind in Anhang 2 des ParlG aufgeführt. Artikel 48 ist bereits in diesem Anhang enthalten. Es ist Sache des Parlaments, bei der Beratung des Gesetzesentwurfs zu entscheiden, ob der neue Artikel 48c hinzugefügt werden soll.

Art. 48d Bearbeitung von Daten und Zusammenarbeit

Abs. 1

Artikel 48d Absatz 1 schafft die gesetzliche Grundlage, damit das BAKOM zur Erfüllung seiner Aufgaben nach den Artikeln 48a und 48b Profilings durchführen und dabei bestimmte besonders schützenswerte Personendaten bearbeiten darf. Diese Aufgaben beinhalten die Erkennung, Bewertung und Abwehr von Cyberbedrohungen sowie den Schutz und die Resilienz von Fernmeldeinfrastrukturen (vgl. Art. 1 Abs. 2 Bst. b und f i. V. m. Art. 48a Abs. 2).

Die dazu erforderlichen besonders schützenswerten Personendaten sind eng begrenzt auf biometrische Identifikationsdaten (vgl. Bst. a) und Daten über verwaltungs- oder strafrechtliche Verfolgungen oder Sanktionen im Fernmeldebereich (vgl. Bst. b). Diese Daten können im Einzelfall notwendig sein, um Cyberangreifer eindeutig zu identifizieren oder Risikoprofile zu erstellen. Eine entsprechende Bearbeitung ist nur zulässig, sofern sie zum Schutz der Fernmeldeinfrastrukturen und vor Cyberbedrohungen erforderlich ist.

Der überwiegende Teil der Cyberbedrohungsanalysen stützt sich jedoch nicht auf Personendaten, sondern auf technische Informationen ohne Personenbezug (z. B. technische Infrastrukturdaten, Malware-Merkmale oder typische Angriffsmuster) beziehungsweise auf Daten über juristische Personen. Die Bearbeitung besonders schützenswerter Daten bleibt somit auf die obgenannten klar umrissenen Ausnahmefälle beschränkt.

Abs. 2

Artikel 48d Absatz 2 erlaubt dem BAKOM, die im Rahmen seiner Aufgaben nach den Artikeln 48a und 48b gewonnenen Daten und Resultate von Profilings an andere für den Schutz vor Cyberbedrohungen zuständige Behörden sowie an nach Artikel 29 anerkannte private und öffentliche Stellen weiterzugeben. Die Weitergabe ist nur zulässig, wenn die empfangende Stelle über eine entsprechende gesetzliche Grundlage verfügt und die Daten zur Erfüllung ihrer Aufgaben im Bereich der Cybersicherheit benötigt. Es handelt sich dabei um Behörden, die ebenfalls im Bereich der Cybersicherheit Aufgaben erfüllen, wie namentlich das BACS, fedpol oder SEPOS.

Die Bestimmung soll sicherstellen, dass der Datenaustausch klar auf den Zweck des Schutzes der Fernmeldeinfrastrukturen und der Abwehr von Cyberbedrohungen begrenzt bleibt (vgl. Art. 1 Abs. 2 Bst. b und f, i. V. m. Art. 48a und 48b) und auch nur von Behörden beantragt werden kann, die selbst einen gesetzlichen Auftrag zum Schutz

⁷⁵ SR 171.10

vor Cyberbedrohungen oder zur Sicherheit oder Resilienz der Fernmeldeinfrastrukturen erfüllen. Eine Bekanntgabe dieser Daten an andere Behörden oder zu anderen Zwecken bleibt ausgeschlossen. Die Bestimmung schafft damit die notwendige Koordinationsgrundlage zwischen dem BAKOM, anderen Behörden und spezialisierten Cybersicherheitsstellen unter Einhaltung der datenschutzrechtlichen Rahmenbedingungen. Personendaten und besonders schützenswerte Personendaten werden nur in den Ausnahmefällen weitergegeben, sofern sie für den Schutz vor Cyberbedrohungen und zur Gewährleistung der Resilienz und der Sicherheit der Fernmeldeinfrastrukturen unbedingt erforderlich sind. Ein Austausch solcher besonders schützenswerten Personendaten dürfte jedoch nur in wenigen Ausnahmefällen vorkommen, da der Grossteil des Datenaustauschs für den Schutz vor Cyberbedrohungen in den allermeisten Fällen, wie in Absatz 1 aufgezeigt, technische Daten betrifft, die keine Identifizierung von Personen erfordern oder zulassen.

Durch die klare Zweckbindung und die Beschränkung auf berechtigte Empfänger trägt Artikel 48d Absatz 2 zu einer wirkungsvollen und rechtmässigen Kooperation bei der Abwehr von Cyberbedrohungen bei.

Abs. 3

Im Rahmen des Wettbewerbes treten die Anbieterinnen von Fernmeldediensten als Konkurrentinnen auf, was grundsätzlich im Sinne des vom FMG angestrebten Wettbewerbs ist. Bei der Bekämpfung von Cyberbedrohungen hingegen sollen Zusammenarbeit und Solidarität vor dem Wettbewerb stehen. Absatz 3 erlaubt den Anbieterinnen daher, untereinander zusammenzuarbeiten, um Informationen, Personendaten, einschliesslich besonders schützenswerter Personendaten und Resultate von Profilings, Ressourcen sowie Fachwissen zu teilen und auf diese Weise gemeinsam die Feststellung und Beurteilung von Bedrohungen, Sicherheitsvorfällen oder einer Gefährdung der Sicherheit, die die Fernmeldeinfrastrukturen betreffen oder betreffen könnten, zu gewährleisten. Dabei kann es um den Wissens- und Erfahrungsaustausch, die gemeinsame Erarbeitung technischer Leitfäden oder sogenannten «*Best Practices*» und vor allem die Schaffung einer gemeinsamen Datenbank gehen. So können rasch und wirksam Informationen über Schwachstellen und andere schwerwiegende Sicherheitsvorfälle, von denen die Anbieterinnen Kenntnis haben, weitergegeben werden.

Abs. 4

Die Analyse oder das Profiling von Cyberbedrohungen, welche die Fernmeldeinfrastrukturen gefährden können (vgl. Art. 48a und 48b), sowie die Resultate von Profilings der entsprechenden Cyberangreifer sind absolut zentral, um die ordnungsgemässe Verwaltung der fernmelderechtlichen Ressourcen und des Funkfrequenzspektrums gegen Cyberangriffe sicherzustellen und diese Fernmeldeinfrastrukturen zu schützen (vgl. Art. 1 Abs. 2 Bst. b und f sowie Art. 48a Abs. 2).

Es ist jedoch äusserst schwierig, im Voraus zu bestimmen, welche Daten für ein Profiling erforderlich und insbesondere welche Formen des Profilings nützlich sind oder künftig nützlich sein werden. Dies hängt von der ständigen und schnellen Entwicklung der Cyberangriffe, der Technologien, der Fernmeldeinfrastrukturen sowie der Vorgehensweisen von Cyberkriminellen ab.

In diesem Kontext sieht Artikel 48d Absatz 4 vor, dass der Bundesrat bei Bedarf im Sinne von Artikel 34 Absatz 3 DSG die Modalitäten der Bearbeitung sensibler Personendaten und des Profilings regeln kann. Es handelt sich hierbei um Bearbeitungen,

die für die Erfüllung einer gesetzlichen Aufgabe unerlässlich sind (vgl. Art. 34 Abs. 3 Bst. a DSGVO), und deren Zweck – der Schutz der Fernmeldeinfrastrukturen und -Ressourcen – für sich genommen kein besonderes Risiko für die Grundrechte der Benutzerinnen und Benutzer darstellt (vgl. Art. 34 Abs. 3 Bst. b DSGVO)

Art. 52 Übertretungen

Abs. 1

Bst. g

Analog zu Artikel 32a Absatz 1 soll der Text mit «Anlagen» (vgl. dazu die Ausführungen zu Art. 32a) ergänzt werden. Zudem wird im deutschen und italienischen Text ein Übersetzungsfehler korrigiert: Es sollte Funkanlagen statt Fernmeldeanlagen heißen. Diese Strafbestimmung deckt alle Straftatbestände im Zusammenhang mit Störsendern ab.

Bst. h

Es ist die Strafbestimmung zum verwaltungsrechtlichen Verbot im Sinne von Artikel 32a Absatz 2 Buchstabe a aufzunehmen: das Funktionsunfähigmachen von Fernmeldeanlagen oder Stark- und Schwachstromanlagen mittels elektromagnetischer Wellen soll unter Strafe gestellt werden (vgl. Erläuterungen zu Art. 32a Abs. 2 Bst. a).

Bst. i

Ebenfalls aufzunehmen ist eine Strafbestimmung zum verwaltungsrechtlichen Verbot im Sinne von Artikel 32a Absatz 2 Buchstabe b: konforme Anlagen können so konfiguriert werden, dass sie die Kommunikation einer gleichartigen Anlage hemmen, sprich vorübergehend verhindern, oder unterbrechen (vgl. Erläuterungen zu Art. 32a Abs. 2 Bst. b). Unter diese Bestimmung fallen nur konforme Fernmeldeanlagen. Im Gegensatz dazu fällt beispielsweise die Nutzung von Störsendern zum Schutz gegen ungewollte Kommunikation bei kulturellen Veranstaltungen nicht unter diese Bestimmung.

Bst. j

Weiter ist eine Strafbestimmung zum verwaltungsrechtlichen Verbot im Sinne von Artikel 34 Absatz 1 aufzunehmen: Das Erstellen und Betreiben von Fernmeldeanlagen mit dem Ziel, den Fernmeldeverkehr oder den Rundfunk zu stören oder zu verhindern, soll unter Strafe gestellt werden. Ebenfalls nicht unter diese Bestimmung fällt beispielsweise die Nutzung von Störsendern.

11. Kapitel: Aufsichtsinstrumente und Verwaltungssanktionen

Im 11. Kapitel soll der Titel des Kapitels angepasst werden, um die materiellen Bestimmungen zweckgerichtet abdecken zu können.

Art. 59 Auskunftspflicht

Abs. 2

Der Ausdruck «amtliche Fernmeldestatistik» wird durch den Ausdruck «Fernmeldestatistik des Bundes» abgelöst, um eine mit dem Bundesstatistikgesetz vom 9. Oktober 1992⁷⁶ (BStatG) abgestimmte Terminologie zu verwenden.

Abs. 2^{bis}

Zur Erstellung von Statistiken gesammelte oder eingereichte Daten dürfen nicht zu anderen Zwecken als den im FMG beschriebenen genutzt werden. Die Liste der Ausnahmen in Artikel 59 Absatz 2^{bis} wurde daher um einen neuen Buchstaben e ergänzt, damit diese Daten zur Aktualisierung der Liste der registrierten Personen im Sinne von Artikel 4 verwendet werden können. Um eine Liste der registrierten Personen auf dem neuesten Stand halten zu können, müssen die bei den statistischen Erhebungen erhaltenen rein administrativen Informationen genutzt werden dürfen, um Aktualisierungen vorzunehmen. So beispielsweise, wenn die Ansprechperson für die Statistik oder die Adresse des Unternehmens geändert hat. Es handelt sich hierbei ausschliesslich um administrative Daten, die der Erstellung der Liste nach Artikel 4 dienen, und keinesfalls um andere Daten, die im Rahmen statistischer Analysen erlangt werden und dem Statistikgeheimnis unterliegen.

Art. 59a Nationaler Breitbandatlas

Das BAKOM sammelt bereits seit mehreren Jahren verschiedene Informationen über die Hochbreitbandversorgung in der Schweiz und veröffentlicht diese in Form von Karten im nationalen Breitbandatlas. Damit dieses für ein systematisches und präzises Monitoring unerlässliche Instrument auf einer umfassenden und langfristigen Grundlage aufgebaut werden kann, muss es künftig für die Erstellung, den Betrieb und die Veröffentlichung des Atlas klare gesetzliche Bestimmungen geben. Diesem Zweck dient der neue Artikel.

Abs. 1

Absatz 1 definiert eindeutig, wer der Mitteilungspflicht unterliegt und bestimmt damit zugleich, welche Art von Informationen übermittelt werden müssen. Die Eigentümerinnen von physischen Fernmeldeleitungen zur Gebäudeerschliessung müssen dem BAKOM regelmässig alle Angaben liefern, die für die Erstellung eines nationalen Breitbandatlas notwendig sind, unabhängig davon, ob sie Fernmeldedienste anbieten oder nicht.

Abs. 2

Die nach dem neuen Artikel 59a erhobenen Daten dienen insbesondere der Erstellung und dem Betrieb eines nationalen Breitbandatlas.

⁷⁶ SR 431.01

Abs. 3

Für die Umsetzung des Entwurfs des Bundesgesetzes über die Förderung des Ausbaus von Breitbandinfrastrukturen (Breitbandfördergesetz, BBFG)⁷⁷ braucht es zusätzliche Informationen zum Netzausbau im Bereich der Internetversorgung in der Schweiz. Damit ersichtlich wird, welche geografischen Gebiete beziehungsweise Gebäude unter Umständen Fördermittel erhalten könnten, ist es wichtig, eine Übersicht zu erstellen und auf einer Karte diejenigen Gebäude anzugeben, die keine Infrastruktur für einen Internetzugang mit einer Bandbreite von mindestens 1 Gbit/s für den Download aufweisen und für die in den nächsten drei Jahren zudem auch kein entsprechendes Ausbauprojekt geplant ist. Nur auf der Grundlage von detaillierten, in nicht aggregierter Form verfügbaren Daten sind die lokalen Behörden in der Lage, zu entscheiden, ob es sich für sie lohnt, vertiefte Untersuchungen und je nach den Ergebnissen ein Ausschreibungsverfahren durchzuführen. Daher soll das BAKOM die Daten, die es für ein möglichst genaues Bild des Netzausbaus für zweckdienlich erachtet, in nicht aggregierter Form veröffentlichen dürfen. Im längerfristigen Interesse der Konsumentinnen und Konsumenten sollte diese Befugnis auch nach dem Erreichen der Ziele des BBFG bestehen bleiben.

Abs. 4

Der Bundesrat legt fest, welche Informationen in welcher Form und in welchem zeitlichen Abstand bereitzustellen sind.

4.2 Durch das Bundesgesetz über die Förderung des Ausbaus von Breitbandinfrastrukturen (BBFG) vorgeschlagene Änderungen des FMG

Der am 14. März 2025 zur Vernehmlassung unterbreitete Vorentwurf des BBFG⁷⁸ enthält drei neue Bestimmungen, die in das FMG aufgenommen werden sollen. Es handelt sich um Artikel 4a (Meldepflicht), Artikel 39a (Verwendung von Konzessionsgebühren) und Artikel 59a (Mitteilungspflicht für einen nationalen Breitbandatlas).

Das BBFG bezweckt, eine weitgehend flächendeckende Versorgung von Wohnungen und Geschäften mit Festnetzanschlüssen zu erreichen, die Übertragungsraten von mindestens 1 Gbit/s für den Download gewährleisten, wozu unter bestimmten Voraussetzungen öffentliche Fördermittel eingesetzt werden können. Dabei soll ein finanzieller Beitrag zum Ausbau von passiven Infrastrukturen zur besseren Versorgung ausschliesslich in Gebieten möglich sein, in denen die Nachfrage nach solchen Leistungen nicht mit dem aktuellen Zugangsnetz gedeckt werden kann und dessen Ausbau innerhalb eines angemessenen Zeithorizonts aufgrund fehlender Rentabilität nicht geplant ist.

Um herauszufinden, wo Handlungsbedarf besteht, müssen in einem ersten Schritt alle Gebäude identifiziert werden, die bestimmte Vorgaben erfüllen⁷⁹ und deren Bewohnerinnen und Bewohnern keine Leitung mit einer Übertragungsrate von 1 Gbit/s für den Download als Internetzugang zur Verfügung steht, weder jetzt noch in den nächsten drei Jahren. Ähnlich wie in den Mitgliedstaaten der EU werden diese Gebäude in Karten

⁷⁷ Siehe abgeschlossene Vernehmlassungen 2025 https://fedlex.data.admin.ch/eli/dl/proj/2025/4/cons_1.

⁷⁸ Siehe abgeschlossene Vernehmlassungen 2025 https://fedlex.data.admin.ch/eli/dl/proj/2025/4/cons_1.

⁷⁹ Damit die Fördermittel möglichst gezielt eingesetzt werden, ist es sinnvoll, alle nicht dauerhaft beheizten oder als Anbauten geltenden Gebäude, z. B. Garagen, Reservoirs, Silos oder Lager, von der Gesamtmenge der in der Schweiz erfassten Gebäude auszunehmen.

ausgewiesen, was eine detaillierte und effiziente Darstellung ermöglicht. Diese Informationen liefern eine grobe Übersicht und ermöglichen den lokalen Behörden abzuwägen, ob es sich im Hinblick auf die Bezeichnung eines möglichen Fördergebiets lohnt, weitere Untersuchungen durchzuführen oder nicht.

Ein solches Kartierungsinstrument ist auf Bundesebene mit dem Breitbandatlas bereits vorhanden, denn das BAKOM sammelt von Unternehmen freiwillig bereitgestellte Daten und veröffentlicht zweimal jährlich Karten, auf denen der Stand des Breitbandausbaus angezeigt wird.⁸⁰ Dennoch muss dieser Atlas vervollständigt und weiterentwickelt werden, indem insbesondere eine Pflicht zur Bereitstellung von Daten für alle Eigentümerinnen von fernmeldetechnischen Infrastrukturen zur Gebäudeerschliessung eingeführt wird, damit die Umsetzung der Strategie zur Förderung des Breitbandausbaus gelingen kann. Durch diese vorgesehenen Änderungen werden die Kenntnis der tatsächlichen Versorgungssituation in der Schweiz und deren Monitoring erheblich verbessert. Dies ist nicht nur für die Verwirklichung der Strategie von Nutzen, sondern auch langfristig, wenn das Programm einmal endet. Dank der neuen Artikel 4a und 59a soll der Atlas somit aktuelle, aussagekräftige und noch genauere Daten liefern, die für die Information der Bevölkerung und der Wirtschaft wesentlich sind und die es den Behörden gestatten, die Wirksamkeit der umgesetzten öffentlichen Massnahmen zu bewerten.

Ausserdem soll die im Rahmen des Breitbandfördergesetzes (vgl. Art. 7 E-BBFG) vorgeschlagene Zweckbindung der Konzessionsgebühren von Funkkonzessionen mit der heutigen Verwendung von Konzessionsgebühren für die Finanzierung begleitender Massnahmen im Zusammenhang mit funkbasierten Technologien (vgl. Art. 39a) abgestimmt werden.

Die Kommentare zu diesen Bestimmungen befinden sich in den entsprechenden Artikeln.

4.3 Änderung eines anderen Erlasses: Bundesgesetz betreffend die elektrischen Schwach- und Starkstromanlagen (Elektrizitätsgesetz, EleG)

Das BAKOM ist zuständig für die Marktaufsicht im Bereich elektrische Geräte im weiteren Sinne, das heisst Geräte und ortsfeste Anlagen, soweit es um Aspekte der elektromagnetischen Verträglichkeit (EMV) geht. Da die Rechtsgrundlage für die Regelung der EMV sehr vage ist, soll die Gelegenheit wahrgenommen werden, eine klare Delegationsnorm im Gesetz zu verankern. Zudem können mehrere Bestimmungen dieses Gesetzes auf den neuesten Stand gebracht werden (vgl. Art. 3, 21 und neu 26b EleG). So soll Artikel 3 Absatz 2 Buchstabe d EleG erweitert und mit den neuen Absätzen 2^{bis} und 2^{ter} ergänzt werden, um dem Bundesrat die Regelung der wichtigsten Grundzüge der Anforderungen an die EMV zu übertragen (analog zu Art. 31 FMG). Sodann geht es nicht nur um den Schutz des Fernmeldeverkehrs, sondern auch um diejenigen der Stark- und Schwachstromanlagen vor elektromagnetischen Störungen. Weiter wird die Verteilung der Kompetenzen in den Artikel 21 Absatz 2 und Artikel 22 EleG ebenfalls klar geregelt. Diese Verteilung entspricht der aktuellen Situation, da das BAKOM bereits heute für die Durchsetzung der Rechtsvorschriften im EMV-Bereich zuständig ist. Zudem werden dem BAKOM die gleichen Kompetenzen und Rechte im Fall von Störungen wie in Artikel 34 Absatz 2 und 34a Absatz 1, 1. Satz in der Fassung des vorliegenden Vorschlages erteilt.

⁸⁰ BAKOM (2025a)

5 Auswirkungen

5.1 Auswirkungen auf den Bund

Im Bereich der Sicherheit entsteht kein personeller oder finanzieller Mehraufwand für den Bund. Durch die Einführung der Artikel 6a und 6b können die Behörden Nummern und Domain-Namen schneller sperren lassen. Angesichts der zunehmenden Zahl von mutmasslichen Straftaten, die über Telefonnummern und Domain-Namen begangen werden, stellt dies eine Steigerung der Verwaltungseffizienz dar.

Die Massnahmen zur Unterstützung des Infrastrukturausbaus haben ebenfalls keinen personellen oder finanziellen Mehraufwand zur Folge.

Die erweiterte Registrierungsmöglichkeit für Anbieterinnen mit einem Angebot von Fernmeldeinfrastrukturen oder -diensten nach Artikel 4 führt zu vernachlässigbarem Aufwand angesichts der geringen Zahl neu zu registrierender Unternehmen und im Hinblick auf das vereinfachte Verfahren, das eingeführt werden soll⁸¹.

5.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Es entstehen nur im Bereich der Sicherheit, insbesondere hinsichtlich der Notkommunikation, relevante Auswirkungen. Indirekt werden in den Artikeln 20 bis 20e die zu meist kantonal betriebenen Zentralen der Notdienste adressiert. Sie sind Teil des Systems Notkommunikation und deshalb besonders von der Umsetzung der Systemaufgaben betroffen. Aufgrund der bereits für den Dienst der Standortidentifikation erfolgten Umstellung auf die neusten Standards der Notkommunikation (*Next Generation 112*, NG112)⁸² und der vom Bundesrat⁸³ auf Stufe FDV geplanten Einführung von SIP-basiertem Echtzeittext (RTT) kann teilweise von Sowieso-Kosten ausgegangen werden. Jedoch könnten bei der Anbindung an Fernmeldenetze Zusatzkosten entstehen, beispielsweise falls die Zentralen nicht bereits durch mehrere Anbieterinnen von Fernmeldediensten erschlossen sind⁸⁴ oder falls gemäss der noch festzulegenden Detailkonfiguration des nach Artikel 20a Absatz 1 Buchstabe a vorgesehenen ESnet neue Anforderungen an die Anbindung der Zentralen entstehen. Gleichzeitig profitieren die ebenfalls kantonal sowie kommunal getragenen Behörden und Organisationen für Rettung und Sicherheit (BORS) von einer resilienteren Notkommunikation.

5.3 Auswirkungen auf die Volkswirtschaft

5.3.1 Sicherheit

Ergänzung der Artikel 6a und 46a, neuer Artikel 6b

Im Rahmen der vorgeschlagenen Konsumentenschutzbestimmungen müssen Anbieterinnen von Telefoniediensten und Domain-Registerbetreiberinnen nach den Artikeln 6a und 6b eine Telefonnummer, einen Internetzugang oder einen Domain-Namen sperren, wenn dieser missbräuchlich verwendet wird. Für die Unternehmen entstehen

⁸¹ Die Auswirkungen der Registrierungspflicht nach Artikel 4a FMG sind in den Unterlagen zum BBFG festgehalten: https://fedlex.data.admin.ch/ei/dl/proj/2025/4/cons_1.

⁸² *Swisscom (2025b)*

⁸³ *Bundesrat (2025b)*

⁸⁴ Vgl. Massnahme M3 im Referenzmodell Notrufe: *UVEK und KKJPD (2022)*.

dadurch keine zusätzlichen Regulierungskosten, da die Sperrungen teilweise bereits heute vorgenommen werden.

Die Aufklärung zu Möglichkeiten im Bereich des Jugendschutzes nach Artikel 46a umfasst Beratung im Shop, online oder telefonisch. Es wird hauptsächlich mit einem einmaligen Mehraufwand für Anbieterinnen von Internetzugängen gerechnet (Aufbereitung Online-Schulung / Recherche-Tools, Apps usw.). Eine Schätzung für die Branche (Anbieterinnen von Internetzugängen) geht von einmaligen totalen Kosten zwischen 120'000 und 240'000 Franken aus. Abhängig von der Nachfrage auf Seiten der Erziehungsberechtigten wird mit jährlich wiederkehrenden Kosten (Beratung, Online-Schulung) von 80'000 bis 650'000 Franken gerechnet. Es sind circa 150 Anbieterinnen von Internetdiensten⁸⁵ betroffen. Wenn keine Branchenlösung realisiert wird, werden die Kosten höher geschätzt. Es wurde zudem geprüft, ob die betroffenen Unternehmen durch die Aufhebung von Regulierungen im gleichen Bereich entlastet werden können. Im Bereich des Schutzes von Kindern und Jugendlichen vor Pornografie kann auf keine bestehende Regulierung verzichtet werden.

Anpassung von Artikel 20 sowie neue Artikel 20a bis 20e

Fernmeldenetze sind kritische Infrastrukturen. Im Rahmen der nationalen Strategie des Bundesrates⁸⁶ zum Schutz kritischer Infrastrukturen gilt die Telekommunikation als Teilsektor von sehr grosser Kritikalität, insbesondere weil andere kritische Infrastrukturen massgeblich von Fernmeldediensten abhängig sind⁸⁷.

Dabei nimmt die Notkommunikation innerhalb der Telekommunikation für die Bevölkerung und die Wirtschaft eine zentrale Rolle ein. In der Schweiz wurden 2023 gemäss BAKOM⁸⁸ rund 3,9 Millionen Notrufe abgesetzt. Diese dienen insbesondere der Alarmierung der Feuerwehr, der Rettungsdienste bei medizinischen Notfällen und der Polizei bei Gefährdungen der öffentlichen Ordnung und Sicherheit. Diese Alarmierungsmöglichkeit ist sowohl in der ordentlichen Lage als auch während Krisen⁸⁹ zum Schutz von Leib und Leben sowie von Eigentum wichtig.

Durch die vorliegenden Massnahmen zur Erhöhung der Resilienz und Verfügbarkeit der Notkommunikation können ausfallbedingte Kosten vermieden werden. In der ordentlichen Lage kann mit jeder gewonnenen Minute pro Einsatz der BORS je nach Annahmen und Einsatztyp ein Nutzenwert von mehreren Tausend Franken resultieren⁹⁰. Zudem zeigen quantitative Abschätzungen zu den Kosten von Unterbrüchen der Stromversorgung (regionale *Blackouts* sowie nationale Strommangellagen gemäss dem Bundesamt für Bevölkerungsschutz, BABS)⁹¹, dass die Aufrechterhaltung verschiedener Fernmeldedienste (Notruf, Sprachanrufe, eingeschränktes Internet, Radio/TV) einem Nutzen von rund 16 Milliarden Franken entsprechen kann. Davon entfallen 30 Prozent allein auf die Aufrechterhaltung von Notrufen⁹².

⁸⁵ Zahlen von 2023 gemäss BAKOM (2025b)

⁸⁶ Bundesrat (2023c)

⁸⁷ BABS (2024) und BfS (2023)

⁸⁸ BAKOM (2025c)

⁸⁹ ETC (2022)

⁹⁰ siehe z. B. Jaldell, Henrik (2017) sowie Weinholt, Åsa / Andersson Granberg, Tobias (2015)

⁹¹ BABS (2020)

⁹² AWK und INFRAS (2022)

Kostenseitig sind vorab die Regulierungskosten für Unternehmen relevant. Die Massnahmen nach Artikel 20e sind gemäss Absatz 4 erst noch zu konkretisieren. Hingegen wurden die aus den Änderungen an Artikel 20 sowie dem neuen Artikel 20a entstehenden Regulierungskosten auf Basis einer Umfrage des BAKOM⁹³ teils quantitativ grob abgeschätzt. Sie werden nachfolgend je Massnahme (vgl. Kapitel [1.2.1](#)) näher beschrieben:

- Die gemäss Artikel 20a vorgesehene Mandatierung für den Betrieb eines ESInet⁹⁴ hätte für die rund 100 Anbieterinnen des öffentlichen Telefondienstes⁹⁵ einmalige Kosten in der Höhe von insgesamt rund 47,2 Millionen Franken⁹⁶ zur Folge. Bei einem vollständig redundanten Betrieb könnten sich diese auf rund 94,4 Millionen Franken erhöhen. Die Kosten entstehen zum weitaus grössten Teil für neue IT-Systeme sowie für den Anschluss von Zentralen der Notdienste und bei der Interkonnektion mit anderen Anbieterinnen von Fernmeldediensten (Konfiguration, Integration usw.). Zu einem kleineren, aber dennoch beträchtlichen Teil entstehen sie für Prozessanpassungen, Testabläufe und Personalschulung. Weiter entstehen rund 8,7 Millionen Franken jährlich wiederkehrende Kosten. Bei einem vollständig redundanten Betrieb könnten sich diese Kosten auf rund 17,4 Millionen Franken erhöhen. Die Kosten entstehen wiederum insbesondere für IT-Systeme (wiederkehrende Lizenzgebühren, Rechenzentrumsleistungen oder Abschreibungen und Ersatzinvestitionen) sowie für Personal und Monitoring/Testabläufe.

- Der gemäss Artikel 20a vorgesehene Betrieb einer Koordinationsstelle für akute Notkommunikationsanliegen könnte zu einmaligen Kosten von 4,2 Millionen Franken sowie jährlich wiederkehrenden Personalkosten von rund 1,1 Millionen Franken führen. Die Kosten würden insbesondere bei der Anbindung an bestehende Operationszentren, bei der Datenanalyse sowie beim für die Koordination notwendigen Personal anfallen.

- Die gemäss Artikel 20a vorgesehene Datenerhebung durch die Betreiberin des ESInet könnte zu einmaligen Kosten von rund 0,5 Millionen Franken sowie jährlich wiederkehrenden Kosten von 0,7 Millionen Franken führen. Die Kosten dürften insbesondere für Software zur Datenerhebung und -auswertung anfallen.

- Die Kosten des ebenfalls in Artikel 20a vorgesehenen Betriebs der Test- und Integrationsplattform wurden nicht quantitativ abgeschätzt, da diese Massnahme erst nach Abschluss der Umfrage aufgenommen wurde. Es dürften Kosten in einstelliger Millionenhöhe entstehen. Diese sollen nach Artikel 20c auch von den Benutzenden dieser Plattform getragen werden.

⁹³ BAKOM (2025d)

⁹⁴ Gemäss dem Standard in *ETSI (2023)*, wobei voraussichtlich nicht ein vollständig autonomes Netz mandatiert wird. Bei einem solchen Netz könnten die Kosten gut um den Faktor 10 höher liegen. Weiter wird in der Schweiz entgegen diesem Standard der Server mit den Informationen zur Standortidentifikation (LIS) zentral durch die Grundversorgungskonzessionärin betrieben. Die Kosten zum LIS werden als Sowieso-Kosten behandelt. Die Kosten gewisser Anbietererschliessungen sowie von einzelnen Netzkomponenten sind aktuell nicht bezifferbar und folglich nicht enthalten. Schliesslich ist absehbar, dass der genannte Standard bis zur Mandatierung durch eine neue Version ersetzt wird. Dieser könnte zusätzliche Komponenten beinhalten und bei der Implementierung entsprechende Mehrkosten verursachen.

⁹⁵ Gemäss *BAKOM (2025b)*. Die Kosten der Systemaufgaben würden gemäss Artikel 20a Absatz 5 anteilmässig zu den abgesetzten Einheiten Notkommunikation auf diese Anbieterinnen umgelegt.

⁹⁶ Hier und nachfolgend handelt es sich um grobe, von diversen Annahmen und noch festzulegenden Anforderungen abhängige Schätzungen. Die Unsicherheit in Bezug auf die (gemittelten) Schätzwerte ist auch aufgrund der grossen Komplexität, des geringen Umfragerücklaufs und der hohen Schwankungsbreite in den Antworten hoch. Die Werte können nur als grobe Orientierung dienen.

- Die gemäss Artikel 20 vorgesehene Einführung einer minimalen Rückfallebene gemäss dem Referenzmodell Notrufe des UVEK und der KKJPD⁹⁷ würde ebenfalls die rund 100 Anbieterinnen von Telefonie betreffen und könnte zu einmaligen Kosten von 32,5 Millionen Franken sowie jährlich wiederkehrenden Kosten von insgesamt rund 4,9 Millionen Franken führen. Jeder Anbieterin würden insbesondere Softwarekosten entstehen für die Verbindung mit den jeweiligen Erschliessungspartnern der Zentralen der Notdienste.

Entlastungsmöglichkeiten für Unternehmen in den übrigen Bereichen der Notkommunikation sind aktuell nicht erkennbar. Die bestehende Regulierung basiert zu einem grossen Teil auf internationalen Standards. Sie muss auch für Touristen und internationale Geschäftsreisende funktionieren, welche ausländische Geräte und Provider nutzen.

Ergänzung der Artikel 32a, 32b, 34 und 34a und 52 sowie von Artikel 3, 21, 22 und 26b EleG

Durch die Verpflichtung der Anbieterinnen, Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten nach Artikel 34 Absatz 1 zur Verfügungstellung der Gesamtheit der relevanten technischen Informationen der betroffenen Anlage wird es möglich sein, sporadisch immer wieder auftretende Störungen (vor allem durch adaptive Antennen), welche die Anbieterinnen, Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten dem BAKOM melden, gezielter aufzufinden und somit beheben zu können. Es ist zu erwarten, dass den Anbieterinnen, Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten dadurch gewisse Kosten entstehen. Diese dürften sich jedoch in einem vernünftigen Rahmen halten, da die gewünschten technischen relevanten Daten vorhanden sein sollten. Zudem dient diese Verpflichtung auch direkt den Anbieterinnen, Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten. Es kann nicht ausgeschlossen werden, dass sie selbst für die Störungen verantwortlich sind.

Mit der Ergänzung von Artikel 52 Absatz 1 Buchstabe j kann die Wirksamkeit der Marktaufsicht erhöht werden. Eine Sanktionsmöglichkeit bei einer zweckbestimmten Störung durch andere Fernmeldeanlagen und Vorrichtungen als solche, die dazu bestimmt sind zu stören, wird wiedereingeführt.

Ergänzung von Artikel 48a sowie neue Artikel 48b und 48c

Die meisten der geplanten Massnahmen im Bereich der Sicherheit und Resilienz der Fernmeldeinfrastrukturen betreffen in erster Linie die drei grossen Anbieterinnen von Fernmeldediensten (Swisscom, Sunrise und Salt). Die Vorgabe zur Mehrlieferantenstrategie dürfte dabei die kostenintensivste Massnahme darstellen. In gewissen Fällen könnten Kosten zur Verringerung der Abhängigkeit eines einzelnen Herstellers anfallen. Die Kosten der Mehrlieferantenstrategie können aber nicht abgeschätzt werden. Entscheidend wird sein, welche Kosten der Herstellerwechsel bzw. der Umstieg auf mindestens zwei Hersteller mit sich bringt. Auch der daraus entstehende Vorteil kann nicht mit vernünftigem Aufwand beziffert werden. Die Anbieterinnen modernisieren und sichern ihre Netze aus eigenem Interesse und auf eigene Kosten, womit von einem grossen Anteil an Sowieso-Kosten zu rechnen ist. Zudem bestehen auch international

⁹⁷ UVEK und KKJPD (2022)

verschiedene Sicherheitsanforderungen (z. B. die «5G-Toolbox» der EU⁹⁸). Entsprechend sollte die Akzeptanz der Branche vorliegen.

Die weiteren Massnahmen sind von geringerer Bedeutung und könnten einige hundert Anbieterinnen von Fernmeldediensten in der Schweiz treffen. Die allermeisten dieser Anbieterinnen erfüllen die operativen und sicherheitstechnischen Anforderungen bereits jetzt, sodass die wirtschaftlichen und finanziellen Folgen für sie begrenzt ausfallen dürften. Im Gegenzug stellt die Sicherung der Fernmeldeinfrastrukturen einen zentralen Wettbewerbsvorteil für den Wirtschaftsstandort Schweiz dar.

Die langfristigen Auswirkungen auf die Produktivität sind derzeit schwierig abzuschätzen, dürften aber tendenziell positiv sein, da die Massnahmen generell die Betriebssicherheit stärken und dadurch Kosten durch Betriebsausfälle vermieden werden könnten.

Zusätzliche Kosten, die sich aus den Massnahmen ergeben, werden mit grosser Wahrscheinlichkeit an die Konsumentinnen und Konsumenten weitergegeben werden.

Die Einführung von Massnahmen zur Sicherung der Fernmeldeinfrastrukturen könnte die Innovation im Bereich der Sicherheit und der Resilienz durch die betroffenen Schweizer Unternehmen stärken und die Digitalisierung vorantreiben.

Die Massnahmen sollen wettbewerbsneutral ausgestaltet werden, sodass keine Einflüsse auf den Wettbewerb in der Schweiz zu erwarten sind.

5.3.2 Infrastrukturausbau

Bei den technischen Vorschriften zur gebäudeinternen Verkabelung in Artikel 35b ist von einem relativ geringen, nicht quantifizierbaren Nutzen auszugehen. Netzbetreiberinnen, die bestehende gebäudeinterne Kabel mitbenutzen wollen, finden damit gleiche Bedingungen vor, was zu geringeren Koordinationskosten und mehr Effizienz bei der Installation führen kann. Zudem kann die Nutzbarkeit für Dritte sichergestellt und eine ineffiziente Duplizierung der gebäudeinternen Verkabelung vermieden werden. Im Allgemeinen ist zwar aufgrund fraglicher Rentabilität⁹⁹ nicht von einer sehr grossen Zahl von Gebäuden auszugehen, die von mehreren Anbieterinnen von Fernmeldediensten mit eigener Infrastruktur erschlossen werden. Das BAKOM schätzt den Anteil parallel mit Glasfaser erschlossener Gebäude auf aktuell vier Prozent¹⁰⁰. Gleichzeitig ergab die unter Kapitel [1.2.2](#) erwähnte Umfrage¹⁰¹ unter den rund 200 Inhaberinnen von FTTH-Betreibernummern, dass rund ein Viertel dieser Unternehmen das in Artikel 35a vorgesehene Recht, weitere Anschlüsse zu den bereits Bestehenden installieren zu können, bereits in Anspruch nahm. Zudem wurde in der Umfrage auf bautechnische Probleme bei der Erschliessung von Mehrfamilienhäusern durch mehrere Netzbetreiberinnen hingewiesen.

Kostenseitig dürfte es sich aufgrund der Orientierung an bestehenden und in einer Branchenarbeitsgruppe erarbeiteten technischen Richtlinien des BAKOM¹⁰² grössten-

⁹⁸ EU (2020)

⁹⁹ Siehe z. B. WIK (2019)

¹⁰⁰ BAKOM (2024c)

¹⁰¹ BAKOM (2024a und b)

¹⁰² BAKOM (2012)

teils um Sowieso-Kosten handeln. Eine mögliche Ergänzung im Bereich des Hausanschlusskastens (HAK)¹⁰³ könnte zukünftig gewisse zusätzliche Kosten verursachen. Unter den (groben) Annahmen, dass in der Schweiz noch 1 Million Gebäude mit Glasfaser zu erschliessen sind¹⁰⁴, dass in fünf Prozent der Fälle ein grösserer HAK und damit Mehrkosten von 100 Franken notwendig werden, und dass Gebäudekategorien zukünftig proportional zu ihrem aktuellen Anteil am Gebäudebestand (ohne Einfamilienhäuser¹⁰⁵) mit Glasfaser erschlossen werden, könnten einmalige Investitionskosten von bis zu rund fünf Millionen Franken entstehen. Dies ist wenig im Vergleich mit den gesamten Investitionskosten für zukünftige Glasfasererschliessungen, welche sich gemäss dem Wissenschaftlichen Institut für Infrastruktur und Kommunikationsdienste (WIK)¹⁰⁶ im Milliardenbereich bewegen.

Eine Entlastung durch die Aufhebung von Regulierungen im Bereich der passiven Infrastruktur ist aktuell nicht vorgesehen. Eine Statistik von Swisscom¹⁰⁷ zur Entbündelung und Interkonnektion zeigt, dass das einzige Zugangsprodukt in diesem Bereich (Kabelkanalisationen KKF) eine stetig wachsende Nachfrage aufweist.

5.3.3 Datengrundlagen

Sollte das BAKOM entscheiden, zur Erfüllung seiner Vollzugs- und Evaluationsaufgaben zusätzliche Anbieterinnen von Fernmeldediensten zu registrieren, würde sich die Zahl der betroffenen Anbieterinnen gemäss Schätzungen des BAKOM zufolge auf rund 50 belaufen. Dieser Wert kann als vernachlässigbar betrachtet werden, umso mehr als er kleiner ist als die in der Statistik des BAKOM jährlich beobachtete Schwankung. Jedes Jahr treten etwa 80 Anbieterinnen von Fernmeldediensten neu in den Markt ein und gleich viele verschwinden. Mit dem für die Registrierung eingeführten vereinfachten Verfahren dürfte es für ein Unternehmen schätzungsweise nicht länger als eine halbe Stunde dauern, sich zu identifizieren, was für Unternehmen minimale Kosten bedeutet.¹⁰⁸ Es wird von einmaligen Kosten für die Anbieterinnen von Fernmeldediensten von insgesamt rund 3000 Franken ausgegangen.

In einem zweiten Schritt müsste diese begrenzte Anzahl Unternehmen auch jährlich den Fragebogen der Fernmeldestatistik ausfüllen, der unterschiedliche thematische Abschnitte für die jeweilige auf dem Markt ausgeübte Tätigkeit umfasst. Da bisher in der Regel kleine Unternehmen nicht erfasst wurden, kann von einem geringen Zeitaufwand für die Datenlieferung ausgegangen werden, der mit der Einführung geeigneter Prozesse mit der Zeit noch sinken wird. Schliesslich ist zu unterstreichen, dass diesen Unternehmen nicht eine neue Pflicht auferlegt wird, sondern dass sie sich einige Erhebungen sparen konnten, weil sie nicht identifiziert worden waren. Zudem schätzen die Anbieterinnen von Fernmeldediensten in der Regel die mit der Registrierung einhergehende Sichtbarkeit. Betreffend die Folgen für die Konsumentinnen und Konsumenten wird sich jede Verbesserung der Kenntnis des gesamten Fernmeldemarkts durch die

¹⁰³ Der HAK soll in einem Gebäude derart platziert werden, dass genügend Platz für den HAK eines weiteren Unternehmens vorhanden ist. Falls dies nicht möglich ist, muss ein für eine allfällige Mitbenutzung geeigneter, genügend grosser HAK installiert werden.

¹⁰⁴ Schätzung auf Basis von Daten des Breitbandatlas, Stand Oktober 2024: *BAKOM (2025a)*.

¹⁰⁵ *BfS (2024)*

¹⁰⁶ *WIK (2017)*

¹⁰⁷ *Swisscom (2024)*

¹⁰⁸ Zudem gilt für die meisten Eigentümerinnen von Infrastrukturen gemäss dem im Entwurf des BBFG vorgesehenen neuen Artikel 4a bereits eine Meldepflicht beim BAKOM.

staatlichen Behörden positiv auf sie auswirken, sei es im Bereich der Regulierung oder der Sicherheit.

5.4 Auswirkungen auf die Gesellschaft

Im Bereich der Sicherheitsaspekte respektive des verbesserten Konsumentenschutzes wird aufgrund der schnelleren Sperrung von Telefonnummern und Domain-Namen nach Artikel 6b mit potenziell weniger Betrugsfällen durch schnellere Sperrung von Nummern und Domain-Namen gerechnet. Dasselbe gilt grundsätzlich auch in Bezug auf Artikel 6a.

Erziehungsberechtigte werden Kinder und Jugendliche aufgrund der Ergänzung von Artikel 46a (Beratung zum Schutz von Kindern und Jugendlichen vor pornografischen Inhalten) vor schädlichen Inhalten aus dem Internet besser schützen können als heute. Der effektive Nutzen der Ergänzung von Artikel 46a hängt aber davon ab, ob die Erziehungsberechtigten die Beratung berücksichtigen und später die Apps oder Tools nutzen werden.

Mit der Anpassung von Artikel 34 Absatz 1 können Störaussendungen besser identifiziert werden.

Infolge der Einführung der verschiedenen Sicherheitsmassnahmen nach den Artikeln 48a bis 48d verbessert sich der Schutz der Schweizer Bevölkerung vor Cyberangriffen im Umgang mit Fernmeldediensten sowie die Resilienz der Fernmeldeinfrastrukturen. Falls es nötig sein sollte, kann der Bundesrat die erforderlichen Massnahmen ergreifen und somit zur Sicherstellung dieser beiden Ziele beitragen.

5.5 Andere Auswirkungen

Auswirkungen auf die Umwelt oder andere Auswirkungen sind nicht zu erwarten.

6 Rechtliche Aspekte

6.1 Verfassungsmässigkeit

Die vorgeschlagene Revision stützt sich insbesondere auf Artikel 92 Absatz 1 BV, wonach das Fernmeldewesen Sache des Bundes ist.

Was der Begriff Fernmeldewesen bedeutet, wird vom Stand der Technik mit Blick auf die wirtschaftlichen und gesellschaftlichen Entwicklungen definiert. So zeigt die Entwicklung, dass die Bundesbehörden stets gewillt waren, neue technische Mittel der Informationsübertragung in das Fernmelderegale (wie es früher auch nach Art. 36 aBV der Fall war) einzuschliessen. Erfasst von Artikel 92 Absatz 1 BV sind somit die nach dem geltenden Stand der Technik und dem Angebot im Markt bekannte Formen der fernmeldetechnischen Übertragung von Informationen wie auch die fernmeldetechnischen Aspekte der Internetkommunikation. Dabei bezieht sich die Regelungskompetenz lediglich auf die fernmeldetechnischen Vorgänge im Zusammenhang mit der Kommunikation, nicht hingegen auf die Regelung der Inhalte derselben¹⁰⁹.

Die Ausgestaltung des Fernmeldewesens liegt im gesetzgeberischen Ermessen und umfasst alle Bereiche, die zur Funktionsfähigkeit der Infrastruktur für das gesamte Fernmeldewesen notwendig sind¹¹⁰. Der Gesetzgeber hat somit im FMG nicht nur das Angebot von Fernmeldediensten und die Organisation des Fernmeldemarktes geregelt, sondern auch zahlreiche Vorschriften über die Ressourcen (Frequenzen, Adressierungselemente, Verzeichnisdaten), die Fernmeldeinfrastrukturen (Anlagen, Kabelkanalisationen) und auch über Mehrwertdienste erlassen.

Die im Rahmen dieser Revision anvisierten Schutzmassnahmen zur Resilienz der Fernmeldeinfrastrukturen beruhen massgeblich auf Artikel 92 BV. Darüber hinaus sollen sie aber auch zur Unabhängigkeit der Schweiz beitragen und dadurch der Wahrung der inneren Sicherheit dienen. Die vorliegende Revision stützt sich daher ebenfalls auf Artikel 173 Absatz 2 BV, der dem Bund eine inhärente Kompetenz im Bereich der inneren Sicherheit überträgt. Diese Kompetenz leitet sich aus dem Bestehen des Staates und der Notwendigkeit ab, dass dieser Bestand geschützt werden können muss. Der Bund muss in der Lage sein, diejenigen Massnahmen zu ergreifen und rechtlich zu regeln, die zum Schutz des Staates, seiner Organe, Behörden und Institutionen erforderlich sind.

Der Entwurf enthält aber auch Bestimmungen, die auf eine Verbesserung des Konsumentenschutzes abzielen und dabei insbesondere die Benutzerinnen und Benutzer von Fernmeldediensten vor Cyberbedrohungen schützen sollen. So sieht Artikel 6b vor, dass Anbieterinnen von Fernmeldediensten bei begründetem Betrugsverdacht auf Hinweis von fedpol Schweizer Telefonnummern und Domain-Namen sperren müssen. Diese Sperrmassnahme stellt eine Einschränkung der Kommunikationsfreiheit der betroffenen Personen dar. Wird die Telefonnummer oder der Domain-Name in einem kommerziellen Kontext verwendet, beeinträchtigt sie auch die wirtschaftliche Freiheit dieser Personen. Die in Artikel 6a vorgesehenen Massnahmen zur Sperrung von Internet und Telefonie zielen ebenfalls auf einen Schutz der Bevölkerung vor Einsatz missbräuchlich verwendeter Adressierungselemente. Es bestehen Zweifel, ob eine solche Massnahme auf die in Artikel 92 BV vorgesehenen Kompetenzen gestützt werden kann, auf die in der Präambel des FMG Bezug genommen wird. Artikel 92 Absatz 1 BV ermächtigt den Bund zwar, die Übermittlung von Informationen, das heisst das Senden

¹⁰⁹ Kern, Markus, *Randziffer 6* (2015)

¹¹⁰ Hettich/Steiner, *Randziffer 9* (2023)

und Empfangen von Mitteilungen zu regeln, nicht jedoch Aspekte, die deren Inhalt betreffen. Sperrmassnahmen, die sich auf den Inhalt oder die Nutzung von Mitteilungen beziehen, müssen daher grundsätzlich auf spezifischen sektoriellen Zuständigkeiten beruhen, wie dies beispielsweise im Bereich des Glücksspiels der Fall ist. Andernfalls würde Artikel 92 Absatz 1 BV seine eigentliche Bedeutung verlieren. Artikel 123 BV, der in der Präambel nicht erwähnt wird, könnte nur dann als Grundlage für eine Sperrpflicht dienen, wenn diese eine im Rahmen eines Strafverfahrens angeordnete Zwangsmassnahme darstellt. Handelt es sich hingegen um Massnahmen zur Verfolgung von Straftaten oder zur Feststellung potenzieller Straftaten, fällt die Massnahme unter das kantonale Polizeirecht. Die im Entwurf vorgeschlagenen Massnahmen in Artikel 6a und 6b zielen darauf ab, die Bevölkerung in der Schweiz vor Telefon- und Internetbetrug zu schützen. Der Gesetzgeber hat bereits in einem vergleichbaren Kontext eingegriffen, indem er die Bestimmungen zur Bekämpfung von unlauterer Massenwerbung (Spam) in Artikel 3 Absatz 1 Buchstabe o des Bundesgesetzes vom 19. Dezember 1986¹¹¹ gegen den unlauteren Wettbewerb (UWG) verabschiedet hat. Diese Bestimmungen stützen sich auf die in der Präambel des UWG aufgeführten Kompetenzen, insbesondere auf Artikel 97 BV. Diese Grundlage verpflichtet den Bund, Massnahmen zum Schutz der Konsumentinnen und Konsumenten zu ergreifen. Des Weiteren basieren sie auf Artikel 95 BV, der den Gesetzgeber ermächtigt, Vorschriften über die Ausübung privater Erwerbstätigkeiten zu erlassen. Diese verfassungsrechtliche Grundlage in Artikel 97 BV könnte auch als Grundlage für die in Artikel 6a und 6b vorgeschlagene Massnahme in Betracht kommen. Die Frage der geeigneten verfassungsrechtlichen Grundlage muss jedoch noch eingehend geprüft und im Rahmen der Vorarbeiten zur Ausarbeitung der Botschaft geklärt werden.

6.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Vorlage schafft keine Unvereinbarkeit mit den internationalen Verpflichtungen der Schweiz. So fallen namentlich die geplanten Massnahmen für Fernmeldeanlagen nicht unter das MRA Schweiz-EU und stellen somit keine technischen Handelshemmnisse dar.

Im Rahmen der dem Bundesrat eingeräumten Kompetenz, hinsichtlich einer möglichen Zuspitzung der geopolitischen Lage bei Bedarf geeignete Massnahmen zum Schutz der Fernmeldeinfrastrukturen zu ergreifen (vgl. Art. 48c), könnten Beschränkungen zum oder ein Ausschluss vom Zugang zum Schweizer Markt für Gerätehersteller beschlossen werden, die als problematisch für die Sicherheit unseres Landes gelten oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der ein Sicherheitsrisiko darstellt. Solche Beschränkungen oder ein Ausschluss sind nach Artikel XIV Buchstabe a (Wahrung der öffentlichen Ordnung), XIV Buchstabe c Ziffer iii und XIV^{bis} (Sicherheit) des Anhangs 1B des Abkommens zur Errichtung der Welthandelsorganisation WTO¹¹² (Allgemeines Abkommen über den Handel mit Dienstleistungen GATS), nach Artikel XIV Buchstabe a Ziffer i (Sicherheit) des Anhangs 1A des Abkommens zur Errichtung der WTO (Allgemeines Zoll- und Handelsabkommen, GATT) und nach den Artikeln 2.10, 5.4 und 5.7 (Nationale Sicherheit) des Anhangs 1A.6 des Abkommens zur Errichtung der WTO (Übereinkommen über technische Handelshemmnisse, TBT) zulässig.

¹¹¹ SR 241

¹¹² SR 0.632.20

6.3 Erlassform

Beim FMG handelt es sich um ein Bundesgesetz im Sinne von Artikel 164 Absatz 1 BV. Dessen Teilrevision untersteht dem fakultativen Referendum gemäss Artikel 141 Absatz 1 Buchstabe a BV.

6.4 Unterstellung unter die Ausgabenbremse

Mit der Vorlage werden weder neue Subventionsbestimmungen geschaffen noch neue Verpflichtungskredite oder Zahlungsrahmen beschlossen. Die Vorlage ist somit nicht der Ausgabenbremse gemäss Artikel 159 Absatz 3 Buchstabe b BV unterstellt.

6.5 Delegation von Rechtsetzungsbefugnissen

Die Vorlage ermächtigt den Bundesrat in den nachstehend aufgeführten vorwiegend technischen oder organisatorischen Bestimmungen Vorschriften zu erlassen. Die Delegation an den Bundesrat erlaubt diesem, die gesetzlichen Vorgaben zu konkretisieren, ohne neue Rechte oder Pflichten zu begründen. Es handelt sich somit um einen Rechtsetzungsauftrag zum Erlass von vollziehendem Ausführungs- und Verordnungsrecht. Diese Delegation rechtfertigt sich insbesondere aufgrund des sich rasch ändernden technischen und sicherheitsrelevanten Umfeld. Bei Bedarf müssen die ausführenden und umsetzenden Rechtsgrundlagen zeitnah angepasst werden können. Der Bundesrat behält zudem gestützt auf Artikel 62 Absatz 2 die allgemeine Kompetenz, dem BAKOM den Erlass der erforderlichen administrativen und technischen Vorschriften zu übertragen.

Der Entwurf überträgt dem Bundesrat oder dem BAKOM den Erlass von Ausführungsbestimmungen in den folgenden Bereichen:

- Festlegung der Einzelheiten in Bezug auf die Meldepflicht für Anbieterinnen von Fernmeldeinfrastruktur zur Erschliessung von Gebäuden (vgl. Art. 4a Abs. 2).
- Erlass von technischen und administrativen Vorschriften durch das BAKOM zu den Systemaufgaben und der sich daraus ergebenden Anforderungen (vgl. 20a Abs. 3).
- Festlegung der Einzelheiten betreffend das zu beschaffende System für die automatisierte Erfassung, die Anonymisierungsvoraussetzungen sowie die Aufbewahrungsdauer der Daten (vgl. 34a Abs. 3).
- Festlegung der Einzelheiten durch das BAKOM betreffend die Zurverfügungstellung von Informationen (vgl. Art. 34a Abs. 4).
- Regelung der technischen Einzelheiten der Mitbenutzung und Erlass von technischen und administrativen Vorschriften durch das BAKOM für den Bau und die Installation gebäudeinterner Anlagen (vgl. Art. 35 Abs. 6).
- Festlegung der Einzelheiten betreffend die störungsverursachenden Geräte (vgl. Art. 26 Abs. 3 EleG).

Der vorliegende Entwurf überträgt dem Bundesrat folgende zusätzliche oder geänderte Rechtsetzungskompetenzen:

- Ausdehnung der sinngemässen Geltung von Rechten und Pflichten von Anbieterinnen von Fernmeldediensten für die Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen oder Kabelkanalisationen für die Sicherstellung des wirksamen Wettbewerbs (vgl. Art. 3a Abs. 2).
- Festlegung der Registrierungsangaben und -Ausnahmen für Anbieterinnen von Fernmeldediensten (vgl. Art. 4 Abs. 5).

- Bezeichnung der Fernmeldedienste, über welche die Notkommunikation sicherzustellen ist, Festlegung von Ausnahmen bezüglich der Sicherstellung der Leitweglenkung, der Standortidentifikation und einer minimalen Rückfallebene sowie Nutzung der Ortungsfunktionen von Endgeräten ohne ausdrückliche Zustimmung der Benutzerin oder des Benutzers (vgl. Art. 20 Abs. 3).
- Erlass von technischen und administrativen Vorschriften durch das BAKOM zu den Systemaufgaben und der sich daraus ergebenden Anforderungen (vgl. Art. 20a Abs. 3).
- Festlegung von technischen und organisatorischen Massnahmen zum Schutz der Integrität der Notkommunikation (vgl. Art. 20e Abs. 4).
- Festlegung der Kriterien für die Anerkennung von für Cybersicherheit zuständige anerkannte private und öffentliche Stellen (vgl. Art. 29 Abs. 3).
- Regelung der Einzelheiten der Bearbeitung von besonders schützenswerter Personendaten und der Durchführung von Profilings für die Sicherheit und das Funktionieren des Domain-Namen-Systems sowie für die Zusammenarbeit mit den spezialisierten privaten oder öffentlichen Stellen in diesem Bereich (vgl. Art. 30a Abs. 3).
- Festlegung der Ausnahmen für die Aufhebung der Rufnummernunterdrückung (vgl. Art. 46 Abs. 2).
- Erlass von weiteren Vorschriften zum Schutz von Kindern und Jugendlichen vor den Gefahren, die sich aus der Nutzung der Fernmeldedienste ergeben (vgl. Art. 46a Abs. 2).
- Präzisierung der Massnahmen von Anbieterinnen von Fernmeldediensten, um die unbefugte Manipulation von Fernmeldeinfrastrukturen durch fernmeldetechnische Übertragungen zu bekämpfen, um die Resilienz der Fernmeldeinfrastrukturen zu verbessern und um vor Cyberbedrohungen zu schützen. (vgl. Art. 48a Abs. 4).
- Verbot von sicherheitskritischen Bestandteilen und Veröffentlichung einer Liste der verbotenen Bestandteile durch das BAKOM (Art. 48b Abs. 3).
- Entfernung von Bestandteilen von Herstellern bei geopolitischen Risiken im Falle eines geopolitischen Risikos (Art. 48c Abs. 3).
- Regelung der Einzelheiten der Bearbeitung von besonders schützenswerter Personendaten und der Durchführung von Profilings zum Schutz vor Cyberbedrohungen und zur Sicherheit und Resilienz der Fernmeldeinfrastrukturen (vgl. Art. 48d Abs. 4).
- Festlegung der im Rahmen der Mitteilungspflicht für einen nationalen Breitbandatlas einzureichenden Daten (vgl. Art. 59a Abs. 4).
- Festlegung der grundlegenden Anforderungen im Bereich der elektromagnetischen Verträglichkeit für elektrische Geräten (vgl. Art. 3 Abs. 2 Bst. d EleG).

6.6 Datenschutz

Die geplanten Massnahmen wurden datenschutzrechtlichen Risikoprüfungen unterzogen. Das Ausmass der neuen vorgesehenen Datenbearbeitungen beschränkt sich hauptsächlich auf Daten, die der Resilienz der Fernmeldeinfrastrukturen und dem Schutz vor Cyberbedrohungen dienen, wobei die überwiegende Mehrheit der zu diesen Zwecken bearbeiteten Daten nicht personenbezogener Natur ist. Vielmehr handelt es sich um Sachdaten und Daten über juristische Personen oder unbestimmte Einheiten im Internet. Eine Bearbeitung besonders schützenswerter Personendaten oder die Erstellung von Profilings im Sinne des DSG dürfte nur in Ausnahmefällen erfolgen. Unter diesen Umständen erweist sich eine weitergehende Datenschutz-Folgeabschätzung nicht als notwendig. Sie könnte jedoch bei Bedarf erfolgen, wenn die Bearbeitung der Personendaten auf Verordnungsstufe präzisiert wird.

Soweit die neuen Bestimmungen die Bearbeitung von Personendaten oder Daten juristischer Personen betreffen, stehen sie im Einklang mit den Grundsätzen des DSGVO sowie des RVOG. Für die individuellen datenschutzrechtlich relevanten Massnahmen wird auf die Erläuterungen der betroffenen Bestimmungen in Kapitel [4](#) verwiesen.

7 Abkürzungsverzeichnis

| | |
|--------|---|
| AGCOM | <i>Autorità per le Garanzie nelle Comunicazioni</i> |
| ARCEP | <i>Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse</i> |
| BABS | Bundesamt für Bevölkerungsschutz |
| BACS | Bundesamt für Cybersicherheit |
| BAKOM | Bundesamt für Kommunikation |
| BBI | Bundesblatt |
| BfS | Bundesamt für Statistik |
| BJ | Bundesamt für Justiz |
| BNetzA | Bundesnetzagentur |
| BORS | Behörden und Organisationen für Rettung und Sicherheit |
| CATV | <i>Cable TV</i> |
| CERT | <i>Computer Emergency Response Team</i> |
| ComCom | Eidgenössische Kommunikationskommission |
| DDoS | <i>Distributed Denial of Service</i> |
| DNS | <i>Domain Name System</i> |
| EDA | Eidgenössisches Departement für auswärtige Angelegenheiten |
| EDÖB | Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| EMV | Elektromagnetische Verträglichkeit |
| ENISA | <i>European Network and Information Security Agency</i> |
| ESInet | <i>Emergency Services IP Network</i> |
| ETC | <i>Emergency Telecommunications Cluster</i> |
| ETSI | <i>European Telecommunications Standards Institute</i> |
| FKS | Feuerwehr Koordination Schweiz |
| FTTC | <i>Fiber to the Curb</i> |
| FTTH | <i>Fiber to the Home</i> |
| Gbit/s | Gigabit pro Sekunde |

| | |
|-------|---|
| GNSS | <i>Global Navigation Satellite System GNSS</i> |
| GEREK | Gremium europäischer Regulierungsstellen für elektronische Kommunikation |
| GNSS | <i>Global Navigation Satellite System</i> |
| HAK | Hausanschlusskasten |
| HR | Handelsregister |
| ICANN | <i>Internet Corporation for Assigned Names and Numbers</i> |
| IKT | Informations- und Kommunikationstechnologie |
| IVR | Interverband für Rettungswesen |
| KKJPD | Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren |
| KKPKS | Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz |
| KMU | Kleine und mittlere Unternehmen |
| KVF-N | Kommission für Verkehr und Fernmeldewesen des Nationalrates |
| KVF-S | Kommission für Verkehr und Fernmeldewesen des Ständerates |
| MRA | <i>Mutual Recognition Agreements</i> |
| MVNO | <i>Mobile Virtual Network Operator</i> |
| NCS | Nationale Cyberstrategie |
| NDB | Nachrichtendienst des Bundes |
| NENA | <i>National Emergency Number Association</i> |
| NG | <i>Next Generation</i> |
| OTT | <i>Over-the-Top</i> |
| PTI | Polizeitechnik und -informatik Schweiz |
| RAN | <i>Radio Access Network</i> |
| RTR | Rundfunk und Telekom Regulierungs-GmbH |
| RTT | <i>Real Time Text</i> |
| SECO | Staatssekretariat für Wirtschaft |
| SEPOS | Staatssekretariat für Sicherheitspolitik |

| | |
|-----------|--|
| swisstopo | Bundesamt für Landestopografie |
| TAV | Technische und administrative Vorschriften |
| UVEK | Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation |
| VBS | Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport |
| WiFi | <i>Wireless Fidelity</i> |
| WIK | Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH |

8 Literaturverzeichnis

AWK und INFRAS (2022): Regulierungsfolgenabschätzung Konkretisierung Art. 48a FMG, <https://www.bakom.admin.ch/de/sicherstellung-der-telekommunikation-bei-strommangellagen>, 29.06.2022.

BABS (2023): Nationale Strategie zum Schutz kritischer Infrastrukturen, <https://www.babs.admin.ch/de/nationale-strategie-zum-schutz-kritischer-infrastrukturen>, 19.09.2023.

BABS (2024): Factsheet zum kritischen Teilsektor Telekommunikation, <https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html>, 04.2024.

BAKOM (2012): Technische Richtlinien betreffend FTTH-Installationen in Gebäuden, physikalische Medien der Schicht 1 Ausgabe 3.0, <https://www.bakom.admin.ch/de/arbeitsgruppen-ftth>, 05.03.2012.

BAKOM (2024a): FTTH-Betreibernummer, <https://www.bakom.admin.ch/de/verlegung-der-glasfaser-in-der-schweiz>, letztmals abgerufen am 07.08.2025.

BAKOM (2024b): Umfrage zu Massnahmen zur Begünstigung des Breitbandausbaus, nicht publiziert.

BAKOM (2024c): Evaluation des Schweizer Fernmeldemarktes, <https://www.bakom.admin.ch/de/evaluation-des-schweizer-fernmeldemarktes>, 15.03.2024.

BAKOM (2025a): Breitbandatlas, <https://www.bakom.admin.ch/de/breitbandatlas>, letztmals abgerufen am 25.04.2025.

BAKOM (2025b): Anzahl der Fernmeldedienstanbieterinnen, <https://www.bakom.admin.ch/de/anzahl-der-fernmeldedienstanbieterinnen>, letztmals abgerufen am 07.08.2025.

BAKOM (2025c): Festnetzdienste über Kurznummern über Festnetz- und Mobilfunkanschlüsse, <https://www.bakom.admin.ch/de/festnetzdienste-ueber-kurznummern-ueber-festnetz-und-mobilfunkanschluesse>, letztmals abgerufen am 07.08.2025.

BAKOM (2025d): Umfrage zu Kosten im Bereich Notkommunikation, nicht publiziert.

BfS (2023): Schweizerische Input-Output-Tabelle 2017, <https://www.bfs.admin.ch/bfs/de/home/statistiken/volkswirtschaft/input-output.html>, 05.12.2023.

BfS (2024): Gebäudekategorie, <https://www.bfs.admin.ch/bfs/de/home/statistiken/bauwohnungswesen/gebaeude/kategorie.html>, letztmals abgerufen am 08.08.2025.

BNetzA (2022): Beschwerdeordnung 2022, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Verbraucher/Un-erlaubte_Telefonwerbung/Beschwerdeordnung_2022.pdf?__blob=publication-File&v=2, letztmals abgerufen am 03.03.2026.

BNetzA (2025): Über 150.000 Beschwerden zum Rufnummernmissbrauch im Jahr 2024, <https://bundesnetzagentur.de/1044230>, 15.01.2025. *Bundesamt für Justiz*

(2024): Informationen für Bundesorgane, <https://www.bj.admin.ch/bj/de/home/staat/datenschutz/info-bundesbehoerden.html>, Gesetzgebungsleitfaden Datenschutz, 01.03.2024.

Bundesrat (2023a): Infrastructure numérique. Réduire les risques géopolitiques, Rapport du 15.12.2023 donnant suite au postulat 20.3984 Pult du 14.9.2020, <https://www.uvek.admin.ch/uvek/fr/home/detec/medias/communiqués-de-presse.msg-id-99431.html>, 15.12.2023.

Bundesrat (2023b): Nationale Cyberstrategie (NCS), <https://www.news.admin.ch/newsd/message/attachments/76793.pdf>, 04.2023.

Bundesrat (2023c): Nationale Strategie zum Schutz kritischer Infrastrukturen, <https://www.babs.admin.ch/de/ski>, 16.06.2023.

Bundesrat (2025a): Appréciation annuelle de la menace, Rapport aux Chambres fédérales et au public du 30.4.2025, <https://www.news.admin.ch/fr/newsb/Ai9gAQL-hlpGdgZisH-g-6>, consulté pour la dernière fois le 08.08.2025.

Bundesrat (2025b): Modernisierung Notrufzugang, [news.admin.ch/de/newsb/ACDiWzoUbRaa9KOjqkUSr](https://www.news.admin.ch/de/newsb/ACDiWzoUbRaa9KOjqkUSr), letztmals abgerufen am 07.08.2025.

Emergency Response Centre Agency Finland (2022): 112 - Emergency number in Finland, <https://www.suomi.fi/services/112-emergency-number-in-finland-emergency-response-centre-agency-finland/01a571b5-3eb9-4b49-a27e-ec8427737c5b>, letztmals abgerufen am 07.08.2025.

ETC (2022): Emergency telecommunications preparedness: Return on investments model, https://www.etcluster.org/sites/default/files/documents/0108_ROI_INTRO-DUCTORY%20BRIEF_compressed.pdf, letztmals abgerufen am 07.08.2025.

ETSI (2023): ETSI TS 103 479 V1.2.1, https://www.etsi.org/deliver/etsi_ts/103400_103499/103479/01.02.01_60/ts_103479v010201p.pdf, 03.2023.

ETSI (2025): ETSI members, <https://www.etsi.org/membership>, letztmals abgerufen am 07.08.2025.

EU (2020): Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>, 23.01.2020.

Hettich, Peter / Steiner, Thomas (2023), in: Ehrenzeller, Bernhard / Egli, Patricia / Hettich, Peter / Hongler, Peter/Schindler, Benjamin / Schmid, Stefan G. / Schweizer, Rainer J. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 4. Aufl., Art. 92.

Jaldell, Henrik (2017): How Important is the Time Factor? Saving Lives Using Fire and Rescue Services, Fire Technology Journal, 53, 695–708.

Kern, Markus (2015), in: Waldmann, Bernhard / Belser, Eva Maria / Epiney, Astrid (Hrsg.), Bundesverfassung, Basler Kommentar, Art. 92.

KKPKS, PTI, FKS und IVR (2024): Informationen des Steuerungsausschuss der Organisation Notrufe Schweiz, zum Thema Kommunikation der Europäischen Notrufnummer 112, https://www.144.ch/wp-content/uploads/2024/07/202407116_Infomationsschreiben_Notrufnummer_DE.pdf, 15.07.2024.

McBride, Freddie (2024): NG112 implementation in Europe – Demystifying the ESInet and Next Generation Core Services, <https://eena.org/blog/ng112-implementation-in-europe-demystifying-the-esinet-and-next-generation-core-services-2/>, 27.03.2024.

NCS (2023): Ziel: Sichere und verfügbare digitale Dienstleistungen und Infrastruktur, <https://www.ncsc.admin.ch/ncsc/de/home/strategie/ziele-massnahmen/ncs-ziel-sichere-verfuegbare-digitale-dl-infrastruktur.html>, letztmals abgerufen am 07.08.2025.

NENA (2025): NENA Standards and Documents, <https://www.nena.org/page/standards>, letztmals abgerufen am 07.08.2025.

Schwaab, Jean-Christophe (2023): Pour une souveraineté numérique, Lausanne: Savoir suisse.

Stadt Zürich (2020): Reglement über die Koordination von Bauarbeiten im öffentlichen Grund (Baukoordinationsreglement), <https://www.stadt-zuerich.ch/de/politik-und-verwaltung/politik-und-recht/amtliche-sammlung/7/702/200.html>, 26.02.2020.

Swisscom (2024): Bericht zur Entbündelung und Interkonnektion; https://www.swisscom.ch/content/dam/swisscom/de/ws/documents/D_Entbuendelung/bericht_zur_entbuendelungundinterkonnektion12-2024.pdf, letztmals abgerufen am 08.08.2025.

Swisscom (2025a): Glasfaserabdeckung FTTH, <https://www.swisscom.ch/de/about/netz/netzausbau-karte-glasfaser.html>, letztmals abgerufen am 07.08.2025.

Swisscom (2025b): Standortlokalisierung für Behörden und Organisationen zur Rettung und Sicherheit (BORS) in der Schweiz, https://www.swisscom.ch/de/business/enterprise/angebot/alarmsolutions-ealarm-emergency/sos-data-base.html?srsId=AfmBOopkRSZEREN9QsqPCqNVLWqx-EFT3bF0TiZ-TAdI9Wus5_K2FWFen, letztmals abgerufen am 07.08.2025.

Swisstopo (2024a): Realisierung des Leitungskatasters Schweiz, <https://www.cadastre.ch/de/realisierung-des-leitungskatasters>, 12.06.2024.

Swisstopo (2024b): Erweiterungen, <https://www.cadastre.ch/de/realisierung-des-leitungskatasters#Erweiterungen>, 12.06.2024.

UVEK und KKJPD (2022): Referenzmodell Notrufe, <https://www.bakom.admin.ch/de/notrufdienste>, 10.11.2022. *Weinholt, Åsa / Andersson Granberg, Tobias (2015)*: New collaborations in daily emergency response: Applying cost-benefit analysis to new first response initiatives in the Swedish fire and rescue service, *International Journal of Emergency Services*, 4(2), 177-193.

WIK (2017): Modellierung der Kosten eines flächendeckenden Hochbreitbandnetzes in der Schweiz, <https://www.bakom.admin.ch/de/wirtschaftliche-analysen>, 05.10.2017.

WIK (2019): Parallele Glasfaserausbauten als Möglichkeiten zur Schaffung von Infrastrukturwettbewerb (Nr. 456), <https://www.wik.org/veroeffentlichungen/veroeffentlichung/nr-456-parallele-glasfaserausbauten-als-moeglichkeit-zur-schaffung-von-infrastrukturwettbewerb>, 12.2019.