

An das  
Bundesministerium für Inneres

Mit E-Mail:

[bmi-III-A-4-stellungnahmen@bmi.gv.at](mailto:bmi-III-A-4-stellungnahmen@bmi.gv.at)

Geschäftszahl: 2024-0.601.313

BKA - V (Verfassungsdienst)  
[verfassungsdienst@bka.gv.at](mailto:verfassungsdienst@bka.gv.at)

**Mag. Laura Vitecek**  
Sachbearbeiterin

[LAURA.VITECEK@BKA.GV.AT](mailto:LAURA.VITECEK@BKA.GV.AT)  
+43 1 53115-203901  
Ballhausplatz 2, 1010 Wien

E-Mail-Antworten sind bitte  
unter Anführung der Geschäftszahl an  
[verfassungsdienst@bka.gv.at](mailto:verfassungsdienst@bka.gv.at) zu richten.

Ihr Zeichen: 2024-0.148.142

## **Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz geändert wird; Begutachtung; Stellungnahme**

Zu dem übermittelten Gesetzesentwurf nimmt das Bundeskanzleramt-Verfassungsdienst  
wie folgt Stellung:

### **I. Allgemeines**

Es wird darauf hingewiesen, dass die Übereinstimmung des im Entwurf vorliegenden  
Bundesgesetzes mit dem Recht der Europäischen Union vornehmlich vom do. Bundes-  
ministerium zu beurteilen ist.

Insoweit der Entwurf Bestimmungen betreffend die Verarbeitung personenbezogener  
Daten enthält, wird auf die vornehmliche Zuständigkeit des Bundesministeriums für Justiz  
für rechtliche Angelegenheiten des Datenschutzes verwiesen.

Vorauszuschicken ist weiters, dass die Intensität des Grundrechtseingriffs der im Entwurf in  
Aussicht gestellten neuen (Überwachungs-)Maßnahmen und somit auch die Verhältnis-  
mäßigkeit dieser Maßnahmen maßgeblich von ihrer technischen Umsetzung abhängt.  
Mangels diesbezüglicher Sachkunde können die technischen Umsetzungsmöglichkeiten der  
(Überwachungs-)Maßnahmen keiner Überprüfung durch das Bundeskanzleramt-

Verfassungsdienst unterzogen werden. Die konkrete Beurteilung der technischen Möglichkeiten – sowie die abschließende Beurteilung der Verhältnismäßigkeit der vorgesehenen Maßnahmen – obliegt dem Bundesministerium für Inneres.

Den nachfolgenden Erwägungen liegt die Prämisse zu Grunde, dass die technische Umsetzung (insbesondere die Ausgestaltung und Eigenschaften des Programms, das zur Überwachung von Nachrichten programmiert und in ein Computersystem eingebracht werden soll) entsprechend der Ausführungen in den Erläuterungen zum Entwurf (insb. S 4 f.) möglich ist und in der beschriebenen Weise erfolgt.

## II. Inhaltliche Bemerkungen

### Allgemeines:

Der Verfassungsgerichtshof hob mit Erkenntnis vom 11. Dezember 2019, G 72-74/2019 ua., unter anderem § 134 Z 3a und § 135a der Strafprozeßordnung 1975 – StPO, BGBl. Nr. 631/1975, in der Fassung des Bundesgesetzes BGBl. I Nr. 27/2018, betreffend die Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten durch Installation eines Programms in einem Computersystem ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter, wegen Unvereinbarkeit mit dem Recht auf Achtung des Privatlebens nach Art. 8 EMRK als verfassungswidrig auf.

Zur Zulässigkeit derartiger auf verschlüsselte Inhalte zugreifender Ermittlungsmaßnahmen entwickelte der Verfassungsgerichtshof in dem oz. Erkenntnis unter Bezugnahme auf die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte insbesondere folgende abstrakte Vorgaben (vgl. insb. Rz. 172 f. und 177):

Die eingreifende Maßnahme muss eine hinreichende innerstaatliche Rechtsgrundlage haben, die rechtsstaatlichen Anforderungen genügt, der betroffenen Person zugänglich ist und erkennen lässt, welche Folgen die Maßnahmen für sie hat. Die „Vorhersehbarkeit“ der Maßnahme setzt überdies voraus, dass das Gesetz hinreichend klar und für die Bürger in angemessener Weise erkennbar darlegen muss, unter welchen Bedingungen und Umständen die Behörden befugt sind, auf solche Maßnahmen zurückzugreifen. Der Verfassungsgerichtshof betonte in diesem Zusammenhang, dass angesichts der einem System der geheimen Überwachung inhärenten Missbrauchsgefahr solche Maßnahmen, insbesondere wegen der ständigen Weiterentwicklung der verfügbaren Technik, aufgrund besonders genauer Rechtsvorschriften angewandt werden müssen. Die Bestimmungen haben folgenden zwingenden Inhalt aufzuweisen: (1.) die Art der Vergehen, welche Anlass

zu geheimen Überwachungsmaßnahmen geben können, (2.) eine Beschreibung der Kategorien von Personen, welche der Überwachung unterliegen, (3.) eine zeitliche Begrenzung der Überwachungsmaßnahme, (4.) das Verfahren, welches bei der Prüfung, Verwendung und Speicherung der erlangten Daten eingehalten werden muss, (5.) Vorsichtsmaßnahmen, welche eingehalten werden müssen, wenn die Daten an andere Personen übermittelt werden, (6.) die Umstände, unter welchen die Aufzeichnungen gelöscht oder zerstört werden können bzw. müssen, und (7.) gesetzliche Vorkehrungen zum Schutz vor Missbrauch solcher Überwachungssysteme. Maßnahmen zur systematischen verdeckten Überwachung sind überdies unter unabhängige (in der Regel gerichtliche) Aufsicht zu stellen, um die Rechte der von der Überwachung Betroffenen zu wahren.

Die mit dem gegenständlichen Entwurf vorgesehenen Rechtsgrundlagen für die Überwachung von Inhaltsdaten von Nachrichten sowie von verschlüsselten Nachrichten durch Einbringen eines Programms in ein Computersystem sind an diesen Vorgaben zu messen. Die geplanten Regelungen orientieren sich grundsätzlich an den vom Verfassungsgerichtshof aufgestellten Mindestinhalten für derartige Überwachungsmaßnahmen. Darüber hinaus sind die für Eingriffe in das Grundrecht auf Datenschutz gemäß § 1 Abs. 2 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, geltenden (engeren) Grenzen (vgl. dazu VfGH 14.12.2024, G 352/2021, Rz. 56 ff.) sowie das Fernmeldegeheimnis (Art. 10a StGG) zu beachten.

### **Zu Z 3 (§ 6):**

#### **Zu Abs. 4:**

Z 1 sieht die Aufschiebung des Einschreitens durch die Organisationseinheiten gemäß § 1 Abs. 3 „nach Maßgabe des § 23 SPG“ und Z 2 die Aufschiebung kriminalpolizeilicher Ermittlungen „nach Maßgabe des § 99 Abs. 4 und 5 StPO“ vor. Es ist unklar, in welchem Zusammenhang die im Schlusssatz genannte Einschränkung („soweit ein überwiegendes Interesse an der Erfüllung der Aufgabe nach Abs. 1 oder 2 besteht“) zu den in § 23 SPG und § 99 Abs. 4 StPO normierten Voraussetzungen für einen Aufschub steht. Eine Klarstellung wird angeregt.

**Zu Z 5 (§ 9):****Zu Abs. 2a:**

Es sollte – zumindest in den Erläuterungen – näher dargestellt werden, welche Kenntnisse bzw. Fähigkeiten einen Bediensteten als geeignet und besonders geschult qualifizieren.

**Zu Z 6 (§ 11 Abs. 1):**Z 5:

Die geplante Z 5 ermächtigt die Direktion zum Einsatz technischer Mittel zur Lokalisierung der von diesen mitgeführten Endeinrichtungen einschließlich der Feststellung der dazugehörenden „IMSI“. Da es sich bei dieser Abkürzung nicht um einen allgemein verständlichen Begriff handeln dürfte, wird vorgeschlagen, der Abkürzung bereits im Gesetzestext eine Umschreibung des Begriffs (etwa „internationale Mobilteilnehmerkennung“, vgl. § 53 Abs. 3b des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991; oder „der zur internationalen Kennung des Benutzers dienenden Nummer“; vgl. § 134 Z 2a StPO) voranzustellen.

Z 8 und 9:

1. Die geplanten Z 8 und 9 beinhalten die gesetzliche Grundlage für die auf dem Gebiet des Verfassungsschutzes neuen Maßnahmen der Überwachung von Nachrichten (Z 8) und der Überwachung von Nachrichten, die verschlüsselt gesendet, übermittelt oder empfangen werden, durch Einbringen eines Programms in ein Computersystem (Z 9). Die in Aussicht gestellten Bestimmungen enthalten eine Reihe unbestimmter Begriffe bzw. allgemein gehaltene Anordnungen, die im Lichte der oz. Rechtsprechung des Verfassungsgerichtshofes zur Notwendigkeit des Bestehens einer „hinreichenden innerstaatlichen Rechtsgrundlage“ näher präzisiert werden sollten:

1.1. Die vorgesehenen Z 8 und 9 nehmen – wie Z 5, 6 und 7 – Bezug auf einen „Betroffenen gemäß § 6 Abs. 2“. Es wird nicht verkannt, dass dieser Ausdruck bereits Inhalt des geltenden § 11 Abs. 1 Z 5, 6 und 7 und weiterer Bestimmungen des Staatsschutz- und Nachrichtendienst-Gesetzes ist (vgl. die Erläuterungen zur Stammfassung ErlRV 763 BlgNR 25. GP 8; demnach sind unter „Betroffenen nach § 6 Abs. 1 Z 2 jene natürlichen Personen zu verstehen, bei denen aufgrund bestimmter Anhaltspunkte ein begründeter Gefahrenverdacht besteht, dass sie einen

verfassungsgefährdenden Angriff begehen werden). Im Kontext der im Entwurf in Aussicht gestellten Überwachungsmaßnahmen erscheint jedoch unklar und lässt sich auch den Materialien nicht unmissverständlich entnehmen, ob die zu überwachende Person nur jene sein kann, hinsichtlich derer der Verdacht der Begehung eines verfassungsgefährdenden Angriffs, dessen Verwirklichung zumindest mit bis zu zehn Jahren Freiheitsstrafe bedroht ist, oder nach § 256 StGB besteht, oder jede Person, hinsichtlich derer ein begründeter Gefahrenverdacht für einen verfassungsgefährdenden Angriff jedweder Art besteht. Eine Klarstellung wird angeregt.

1.2. Konkretisierungsbedürftig erscheint auch der Ausdruck in Z 9 „in ein Computersystem [...] eines Betroffenen nach § 6 Abs. 2“. So ist unklar, ob das zu überwachende Computersystem sich im Eigentum bzw. Besitz der betroffenen zu überwachenden Person befinden muss (oder ob auch Computersysteme unbeteiligter Dritter bzw. öffentlich zugängliche Computersysteme einer Überwachung unterliegen dürfen, wenn diese vom Betroffenen genutzt werden). Sofern von der Maßnahme unbeteiligte Dritte erfasst sein sollten, erhöht dies die „Streubreite“ und damit die Intensität des Grundrechtseingriffs und insofern auch die Anforderungen an seine Rechtfertigung im Rahmen der vorzunehmenden Verhältnismäßigkeitsprüfung.

1.3. Die geplante Z 8 sieht als (alternative) Voraussetzung für die Überwachung von Nachrichten vor, dass diese Überwachung „zur Durchführung einer Ermittlungsmaßnahme nach Z 9 erforderlich ist“. Es erscheint fraglich, inwiefern die Überwachung von Nachrichten zur Durchführung der Überwachung von verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten „erforderlich“ sein kann. In den Erläuterungen (vgl. S 5) wird dazu ausgeführt, dass die Überwachung nach Z 8 diesfalls der „Eruierung, welche Kommunikationskanäle der Betroffene nutzt“ dient. In der Folge wird ausgeführt, dass eine Maßnahme nach Z 8 auch in jenen Fällen einsetzbar sein muss, in denen sie selbst hinsichtlich der Inhaltsüberwachung von Nachrichten nicht erfolgsversprechend erscheint, weil beispielsweise durch (verdeckte) Observation bereits festgestellt werden konnte, dass der Betroffene ausschließlich verschlüsselt kommuniziert. Es ist jedoch fraglich, inwiefern eine Überwachung von Nachrichten in diesen Fällen darüber Aufschluss geben kann, welche Applikationen der Betroffene für die verschlüsselte Kommunikation nutzt. Eine Überprüfung und Klarstellung wird angeregt.

1.4. Z 9 ermächtigt zur Überwachung von verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten „durch Einbringen eines Programms in ein Computersystem [...] unter Einsatz technischer Mittel“. Es wird angeregt zu prüfen, ob diese Formulierung im Lichte der Erläuterungen (insbesondere zur technischen Regulier- und

Beschränkbarkeit auf von der gerichtlichen Bewilligung umfasste Nachrichten aus bestimmten Applikationen) konkretisiert werden kann. Es wird darauf hingewiesen, dass die Art und Weise der technischen Umsetzung – insbesondere die Möglichkeit der technischen Beschränkung auf bestimmte Nachrichten bzw. bestimmte Applikationen sowie die mit dem einzubringenden Programm verbundenen Auswirkungen auf das Computersystem – maßgeblichen Einfluss auf die Schwere des Grundrechtseingriffs und damit die Verhältnismäßigkeit der Maßnahme haben kann.

1.5. Die „Überwachung von Nachrichten“ soll nach den Materialien neben der herkömmlichen (Sprach- und SMS-)Telekommunikation sowohl sämtliche Nachrichten und Informationen, die über internetbasierte Apps wie WhatsApp, Telegram etc. übermittelt werden, als auch über einen Cloud-Diensteanbieter an einen Cloud-Server übermittelte Datenpakete umfassen (S 4). Nach den Erläuterungen ist vor der Einbringung der Software in das Computersystem eine Eingrenzung der Zugriffsmöglichkeiten der Software auf bestimmte Kommunikationsapplikationen zu prüfen; weiters ermögliche die Software, dass nur „gezielte und von der Bewilligung umfasste Nachrichten aus bestimmten Applikationen ausgeleitet werden können“ (S 4 f.). Diese Begrenzung des Zugriffs findet jedoch im Gesetzestext keinen Niederschlag (weder die Befugnis zur Überwachung von Nachrichten in § 11 Abs. 1 noch die geplanten Bestimmungen über die gerichtliche Bewilligung in § 15a sehen eine Einschränkung der Maßnahme auf konkrete Applikationen vor). Zudem hängt die Qualifikation der Schwere des Grundrechtseingriffs auch maßgeblich davon ab, welche Nachrichten bzw. Daten eines Computersystems der Überwachung unterliegen. Insofern sollte in den Erläuterungen präzisiert werden, was mit „Datenpaketen“, die „über einen Cloud-Diensteanbieter an einen Cloud-Server übermittelt“ werden, gemeint ist. Sofern von der Überwachung etwa auch regelmäßige „Backups“ im Sinne einer Übertragung der auf einem Computersystem befindlichen Daten (etwa Dateien, Fotos, Videos, Kalendereinträge, Notizen etc.) an einen Cloud-Server betroffen sein können, wäre dies angesichts der möglichen betroffenen Dateninhalte und -mengen bei der Beurteilung der Schwere des Grundrechtseingriffs und bei der Prüfung der Verhältnismäßigkeit entsprechend zu berücksichtigen (vgl. in diesem Sinne zur Notwendigkeit der Beschränkung von Datenkategorien und -inhalten im Rahmen der gerichtlichen Bewilligung bei der Sicherstellung eines Datenträgers VfGH 14.12.2023, G 352/2021, Rz. 79). Eine Überprüfung wird angeregt.

2. Der Verfassungsgerichtshof hat in der oz. Entscheidung betont, dass die verdeckte Überwachung der Nutzung von Computersystemen einen schwerwiegenden Eingriff in die von Art. 8 EMRK geschützte Privatsphäre darstellt und nur in äußerst engen Grenzen zum Schutz entsprechend gewichtiger Rechtsgüter zulässig ist. Sie darf nur dann erfolgen,

wenn sie zur Verfolgung und Aufklärung von Straftaten dient, die im Einzelfall eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darstellen und die einen solchen schwerwiegenden Eingriff rechtfertigen (vgl. VfGH 11.12.2019, G 72-74/2019, Rz. 180 ff). Der Verfassungsgerichtshof kritisierte in dieser Entscheidung, dass die diesem Erkenntnis zu Grunde liegenden Überwachungsmaßnahmen für verschlüsselte Nachrichten nicht nur bei einer drohenden Gefahr schwerer Kriminalität und der Verletzung besonders wichtiger Rechtsgüter, sondern „auch zur Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder terroristischen Vereinigung begangenen oder geplanten Verbrechen gegen das Vermögen“ möglich war (vgl. insb. Rz. 190 vorletzter und letzter Satz).

Vor diesem Hintergrund wird empfohlen, die Verhältnismäßigkeit der vorgesehenen Maßnahmen in den Erläuterungen näher zu begründen und den mit der Überwachungsmaßnahme verbundenen Eingriff mit den (gewichtigen) öffentlichen Interessen an der Vorbeugung von verfassungsgefährdenden Angriffen der genannten Schwere abzuwägen. Zu diesem Zweck sollten nähere Ausführungen zu den einzelnen Deliktgruppen, hinsichtlich derer eine Überwachungsmaßnahme zulässig sein soll, und die durch diese Delikte verursachte gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele aufgenommen werden.

#### **Zu Z 8 (§ 11 Abs. 2 und 3):**

Die Verpflichtung, „an der Überwachung von Nachrichten mitzuwirken“, sollte präzisiert werden; auch sollte klargestellt werden, wen eine derartige Verpflichtung trifft (etwa die Anbieter gemäß § 134 Z 6 StPO im Fall der Überwachung von Nachrichten gemäß der vorgesehenen Z 8; vgl. § 138 Abs. 2 StPO). Unklar ist in diesem Zusammenhang, welche „Stelle“ in welcher Form bei der Überwachung von verschlüsselten Nachrichten durch Einbringen eines Programms in ein Computersystem (Z 9) zur Mitwirkung verpflichtet sein könnte; eine Überprüfung und Klarstellung wird empfohlen.

#### **Zu Z 9 (§ 14):**

##### **Zu Abs. 2:**

Es ist unklar, wie sich der (neu angefügte) letzte Satz zum vorletzten Satz verhält, zumal sich beide Sätze (auch) auf Ermächtigungen gemäß § 11 Abs. 1 Z 7 beziehen. Eine Überprüfung wird empfohlen.

**Zu Z 10 (§ 14):****Zu Abs. 4 und 5:**

1. Der Verfassungsgerichtshof führte im Erkenntnis vom 11. Dezember 2019, G 72-74/2019 ua., aus, dass es in „Anbetracht der Besonderheiten des eingesetzten Mittels und der verdeckten Überwachung sämtlicher über ein bestimmtes Computersystem versendeter, übermittelter oder empfangener Nachrichten über einen längeren Zeitraum [...] einer begleitenden, effektiven – mit entsprechenden technischen Mitteln und personellen Ressourcen ausgestatteten – Aufsicht über die laufende Durchführung [der] Maßnahme durch das Gericht (oder eine mit gleichwertigen Unabhängigkeitsgarantien ausgestatteten Stelle)“ bedarf. Ein durch den Richtervorbehalt gewährleisteter Rechtsschutz bloß zu Beginn, nämlich bei der Bewilligung der Anordnung der Maßnahme reicht „im Lichte der besonderen Qualität der vorgesehenen laufenden verdeckten Überwachung von (Teilen von) Computersystemen unter dem Blickwinkel des Art. 8 EMRK nicht aus“. Die in den dem oz. Verfahren zu Grunde liegenden Bestimmungen vorgesehene Prüfung und Kontrolle der Durchführung der Überwachung durch den Rechtsschutzbeauftragten (gemäß der Strafprozeßordnung 1975) zusammen mit einem Richtervorbehalt vor Beginn der Überwachungsmaßnahme erachtete der Verfassungsgerichtshof als nicht hinreichend (vgl. Rz. 191 ff.).

2. Gemäß dem vorliegenden Gesetzesentwurf soll die laufende Kontrolle und Prüfung der (verdeckten) Überwachung von Nachrichten dem Rechtsschutzbeauftragten gemäß § 91a SPG zukommen. Vor der Beantragung der Bewilligung der Überwachung von Nachrichten nach § 11 Abs. 1 Z 8 und 9 ist der Rechtsschutzbeauftragte zu befassen und ihm Gelegenheit zur Äußerung binnen drei Tagen zu geben. Ihm obliegt außerdem die Prüfung der Bewilligung und die begleitende Kontrolle der Durchführung einer solchen Ermittlungsmaßnahme, wobei er darauf zu achten hat, dass während der Durchführung die Bewilligung nicht überschritten wird und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist. Die Organisationseinheiten der Direktion haben dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen sowie in die Datenverarbeitungen zu gewähren, Abschriften auszufolgen und Auskünfte zu erteilen. Ihm ist jederzeit Gelegenheit zu geben, die Durchführung derartiger Maßnahmen zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden. Zudem hat er die Einhaltung der Pflicht zur Richtigstellung und Löschung von Daten zu überwachen (§ 15 Abs. 1 und 2 SNG). Dem Rechtsschutzbeauftragten steht weiters das Recht zu, gegen die Bewilligung des



Bundesverwaltungsgerichts Revision an den Verwaltungsgerichtshof zu erheben (geplanter § 15a Abs. 4). Nimmt der Rechtsschutzbeauftragte wahr, dass durch die Verarbeitung personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Verarbeitung keine Kenntnis haben, hat er eine Beschwerde an die Datenschutzbehörde nach § 90 SPG zu erheben (§ 16 Abs. 1 SNG). Schließlich ist dem Rechtsschutzbeauftragten nach Beendigung einer solchen Ermittlungsmaßnahme Gelegenheit zu geben, die weiterverarbeiteten Nachrichten einzusehen und anzuhören. Er ist berechtigt, die Löschung von (Teilen von) Nachrichten zu beantragen und sich von der ordnungsgemäßen Löschung zu überzeugen (geplanter § 15a Abs. 9).

Der Verfassungsgerichtshof hat in der oz. Entscheidung weitgehend offengelassen, wie eine begleitende, effektive – mit entsprechenden technischen Mitteln und personellen Ressourcen ausgestattete – Aufsicht über die laufenden Überwachungsmaßnahmen auszugestalten wäre. Die Übertragung dieser Aufgaben der Prüfung und Aufsicht an den Rechtsschutzbeauftragten (der Justiz), der nach den Maßgaben der Strafprozeßordnung 1975 eingerichtet war, und die Befugnisse, die ihm eingeräumt waren, erachtete das Höchstgericht unter Berücksichtigung der Eingriffsintensität der in der Strafprozessordnung vorgesehenen verdeckten Überwachungsmaßnahmen für nicht hinreichend. Der Verfassungsgerichtshof hat in dieser Entscheidung jedoch nicht kategorisch ausgeschlossen, dass die Kontrolle derartiger Überwachungsmaßnahmen durch eine Einrichtung wie den Rechtsschutzbeauftragten vorgenommen wird, solange dadurch eine effektive – mit entsprechenden technischen Mitteln und personellen Ressourcen ausgestattete – Aufsicht gewährt wird (vgl. *Oswald*, Die Verfassungswidrigkeit des „Staatstrojaners“, ÖZW 2020, 85 [95]; aA *Lachmayer*, Rechtsstaatliche Grenzen polizeilicher Überwachungsbefugnisse, Jahrbuch Öffentliches Recht 2020, 105 [117], der hinsichtlich des Sicherheitspolizeigesetzes die Notwendigkeit der Errichtung einer neuen unabhängigen Verwaltungsstelle in den Raum stellt).

3. Das Bundeskanzleramt-Verfassungsdienst geht davon aus, dass durch eine Übertragung der Kontroll- und Aufsichtsbefugnisse auf den (unabhängigen) Rechtsschutzbeauftragten den Vorgaben des Verfassungsgerichtshofes Genüge getan werden kann, sofern dieser über die notwenigen personellen Ressourcen verfügt und ihm effektive Mittel zur Aufsicht zur Verfügung stehen:

3.1. § 91b Abs. 3 SPG normiert (anders als die dem Verfahren G 72-74/2019 zu Grunde liegenden Bestimmungen der Strafprozeßordnung 1975), dass der Bundesminister für Inneres dem Rechtsschutzbeauftragten und seinen Stellvertretern die zur Bewältigung der administrativen Tätigkeit notwendigen Personal- und Sacherfordernisse zur Verfügung zu

stellen hat, wobei diese den jeweiligen gesetzlichen Aufgaben adäquat anzupassen sind. Es wird angeregt, die aufgrund der vorgesehenen neuen Befugnisse zusätzlich erforderlichen Personal- und Sacherfordernisse in den Erläuterungen (bzw. in der noch zu erstellenden wirkungsorientierten Folgenabschätzung) näher darzulegen. Insbesondere wird sicherzustellen sein, dass der Rechtsschutzbeauftragte über die notwendige technische Expertise betreffend die bei der Überwachung von verschlüsselten Nachrichten zum Einsatz kommenden technischen Mittel verfügt.

3.2. Zudem wird angeregt, eine Stärkung der Befugnisse des Rechtsschutzbeauftragten zu prüfen. Die im Staatsschutz- und Nachrichtendienst-Gesetz bereits geregelten in Verbindung mit den im Entwurf vorgesehenen weiteren Kontrollbefugnissen des Rechtsschutzbeauftragten ähneln nämlich weitgehend jenen Befugnissen, die dem Rechtsschutzbeauftragten in der Strafprozeßordnung 1975 in Bezug auf die Inhaltsüberwachung von verschlüsselten Nachrichten eingeräumt wurden:

Dem Rechtsschutzbeauftragten obliegt zwar die begleitende Kontrolle der Überwachungsmaßnahme (§ 14 Abs. 5 des Entwurfs). Stellt er einen Missbrauch der Befugnisse oder eine Rechtsverletzung durch die ermittelnde Behörde fest, stehen ihm allerdings – soweit ersichtlich – nur eingeschränkt Mittel zur Verfügung. Das in § 15a Abs. 4 vorgesehene Recht, gegen die Bewilligung des Bundesverwaltungsgerichts Revision beim Verwaltungsgerichtshof zu erheben, bietet keine Abhilfe gegen allfällige Rechtsverletzungen, die der Rechtsschutzbeauftragte im Rahmen seiner laufenden Kontrolle der Durchführung der Überwachung feststellt (zB Überschreitung der gerichtlichen Bewilligung). Zudem wird der Verwaltungsgerichtshof im Revisionsverfahren nicht als Tatsacheninstanz tätig und ist die Zulässigkeit einer derartigen Revision gemäß Art. 133 Abs. 4 B-VG von der Darlegung einer Rechtsfrage grundsätzlicher Bedeutung (durch den Rechtsschutzbeauftragten) abhängig. Gemäß § 16 Abs. 1 SNG ist der Rechtsschutzbeauftragte darüber hinaus zwar zur Erhebung einer Beschwerde an die Datenschutzbehörde gemäß § 90 SPG verpflichtet, sofern er wahrnimmt, dass durch Verarbeiten personenbezogener Daten Rechte von Betroffenen einer Aufgabe nach § 6 Abs. 1 oder 2 verletzt worden sind. Es scheint jedoch keine Möglichkeit zu bestehen, die Rechtmäßigkeit der Modalitäten der Durchführung der Überwachung durch die Organisationseinheiten einer (gerichtlichen) Kontrolle unterziehen zu lassen.

Vor diesem Hintergrund könnte hinterfragt werden, ob dem Erfordernis der „effektiven Aufsicht und Kontrolle“ im Sinne der Rechtsprechung des Verfassungsgerichtshofes mit dem vorliegenden Entwurf gerecht wird.

**Zu Z 12 (§ 15a):****Zu Abs. 1 und 3:**

Abs. 1 und 3 sehen vor, dass Anträge auf Bewilligung einer Ermittlungsmaßnahme gemäß § 11 Abs. 1 Z 8 oder 9 (Überwachung von Nachrichten) an das Bundesverwaltungsgericht zu stellen sind, das per Beschluss zu entscheiden hat.

Es wird darauf hingewiesen, dass ein Bundesgesetz, das eine derartige Zuständigkeit des Bundesverwaltungsgerichts zur Entscheidung über „Anträge in sonstigen Angelegenheiten“ (vgl. Art. 130 Abs. 2 Z 4 B-VG) vorsieht, gemäß Art. 131 Abs. 4 Z 2 lit. d iVm Abs. 4 letzter Satz B-VG nur mit Zustimmung der Länder kundgemacht werden darf. Darauf wäre auch im (noch zu ergänzenden) Vorblatt und im Allgemeinen Teil der Erläuterungen hinzuweisen.

Soweit in Abs. 1 vorgesehen wird, dass Anträge an das Bundesverwaltungsgericht „im elektronischen Weg über einen sicheren Kommunikationskanal“ zu stellen sind, ist unklar, was unter einem „sicheren Kommunikationskanal“ zu verstehen ist. Dies gilt ebenso für die Zustellung gemäß Abs. 3. Eine Überprüfung wird angeregt.

**Zu Abs. 2:**

Nach den Ausführungen in den Erläuterungen zu § 11 Abs. 1 Z 8 und 9 sowie Abs. 2 und 3 ist die in das Computersystem einzubringende Software technisch regulierbar, sodass nur gezielte und von der Bewilligung umfasste Nachrichten aus bestimmten Applikationen ausgeleitet werden können. Den in Abs. 2 vorgesehenen Inhaltserfordernissen eines Antrags auf Bewilligung zur Durchführung einer Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 oder 9 lässt sich demgegenüber keine derartige Eingrenzung auf bestimmte Applikationen bzw. Kommunikationsdienste entnehmen (vgl. dazu bereits die Anmerkung zu Z 6).

**Zu Abs. 4:**

Der Ausdruck „nach Zustellung des Beschlusses“ sollte entfallen. Derartige das Verfahren des Verwaltungsgerichtshofes (nämlich das für den Lauf der Revisionsfrist maßgebliche fristauslösende Ereignis) betreffende Regelungen sollten mit Blick auf Art. 136 Abs. 4 B-VG, wonach die Organisation und das Verfahren des Verwaltungsgerichtshofes „durch ein besonderes Bundesgesetz“ geregelt werden (vgl. zu diesem „Kodifikationsgebot“:

*Faber*, Verwaltungsgerichtsbarkeit [2013] Art. 136 B-VG, Rz. 8; vgl. zur Revisionsfrist § 26 des Verwaltungsgerichtshofgesetzes – VwGG, BGBl. Nr. 10/1985), unterbleiben.

#### **Zu Abs. 7:**

Abs. 7 berechtigt die „Organisationseinheit gemäß § 1 Abs. 3“ zur Prüfung und Weiterverarbeitung der ermittelten Nachrichten gemäß § 11 Abs. 1 Z 8 und 9. Demgegenüber soll die Antragstellung gemäß Abs. 1 an das Bundesverwaltungsgericht einzig der Direktion Staatsschutz und Nachrichtendienst obliegen. Die Verarbeitung der ermittelten Daten kann demnach auch durch die in jedem Bundesland für Staatsschutz zuständige Organisationseinheit der Landespolizeidirektion erfolgen. Eine Überprüfung wird angeregt.

#### **Zu Abs. 9:**

Nach Abs. 9 ist vorgesehen, dass der Rechtsschutzbeauftragte berechtigt ist, die Löschung von Nachrichten oder Teilen von ihnen „zu beantragen“. Dieser Wortlaut impliziert, dass in diesen Fällen ein (förmliches) Verfahren zu führen und ein Erledigungsanspruch des Rechtsschutzbeauftragten (über seinen Antrag) besteht. Dazu lässt sich den Erläuterungen jedoch nichts entnehmen. Eine Klarstellung bzw. Überprüfung wird angeregt.

#### **Zu Abs. 10:**

Es sollte (zumindest in den Erläuterungen) klargestellt werden, wann davon auszugehen ist, dass der Geschädigte die Durchführung der Ermittlungsmaßnahme vorsätzlich herbeigeführt hat.

#### **Zu Z 13 (§ 16):**

#### **Zu Abs. 2:**

1. Abs. 2 sieht die (nachträgliche) Information der von einer Überwachungsmaßnahme betroffenen Personen durch die Direktion Staatsschutz und Nachrichtendienst vor.

In den Erläuterungen (§ 8) wird darauf hingewiesen, dass der Betroffene gegen den bewilligenden Beschluss des Bundesverwaltungsgerichts Revision an den Verwaltungsgerichtshof nach Maßgabe der §§ 25a ff. VwGG erheben kann. Der

vorgesehene Abs. 2 sieht allerdings keine Zustellung des Bewilligungsbeschlusses des Bundesverwaltungsgerichts (nach Beendigung der Überwachungsmaßnahme) vor (siehe demgegenüber § 138 Abs. 5 StPO). Darüber hinaus wird erneut darauf hingewiesen, dass die Zulässigkeit der Erhebung einer Revision gemäß Art. 133 Abs. 4 B-VG von der Darlegung einer Rechtsfrage grundsätzlicher Bedeutung abhängt und der Verwaltungsgerichtshof grundsätzlich an den vom Bundesverwaltungsgericht festgestellten Sachverhalt gebunden ist. Eine Überprüfung wird empfohlen. Es wird überdies angeregt, in den Erläuterungen auch auf das Recht auf Erhebung einer Beschwerde an den Verfassungsgerichtshof gegen den Bewilligungsbeschluss des Bundesverwaltungsgerichts gemäß Art. 144 Abs. 4 B-VG (iVm § 88a Abs. 1 VfGG) hinzuweisen.

Zudem ist unklar, welche Folgen mit einer allfälligen Aufhebung des Beschlusses des Bundesverwaltungsgerichts verbunden sind (etwa eine unverzügliche amtswegige Lösungsverpflichtung der basierend auf dem aufgehobenen Beschluss ermittelten Daten). Schließlich lässt der Entwurf offen, ob bzw. welche Einsichts- bzw. Lösungsrechte dem Betroffenen (nach seiner Verständigung) zukommen. Eine Überprüfung wird angeregt.

2. Jedenfalls wäre in Abs. 2 im Hinblick auf die Überwachung von Nachrichten gemäß § 11 Abs. 1 Z 8 und 9 nicht auf „die Ermächtigung“, sondern auf die gerichtliche Bewilligung abzustellen. Es sollte überdies geprüft werden, ob nicht – statt auf den Ablauf der Zeit, für die die Bewilligung erteilt wurde – auf die Beendigung der Überwachung an sich abzustellen ist, zumal sich eine Überwachung auch bei aufrechter Bewilligung als nicht mehr erforderlich erweisen kann (und aufgrund des Verhältnismäßigkeitsgrundsatzes diesfalls auch sofort zu beenden wäre). Zudem wird angeregt zu normieren, binnen welcher Frist der Betroffene (bzw. allfällige Dritte) von den Maßnahmen zu informieren sind (wohl: „unverzüglich“; vgl. wiederum § 138 Abs. 5 StPO).

3. Nach dem zweiten Satz sind auch jene Personen, an die oder von denen Nachrichten gesendet, übermittelt oder empfangen wurden, die gemäß Abs. 7 weiterverarbeitet wurden, nachweislich zu informieren, sofern ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist.

Der Ausdruck „ohne besonderen Verfahrensaufwand“ sollte einer Überprüfung unterzogen werden. Es ist nämlich zu berücksichtigen, dass es sich bei der Überwachung von Nachrichten grundsätzlich um einen gewichtigen Eingriff in die von Art. 8 EMRK geschützte Privatsphäre (bzw. das Recht auf Datenschutz) handelt, mit dem Einblick in

sämtliche – auch höchstpersönliche – Lebensbereiche gewonnen werden können (vgl. dazu VfGH 11.12.2019, G 72-74/2019, Rz. 179). Ausgehend davon sollte sichergestellt werden, dass die von der Überwachung betroffenen Personen verständigt werden, um die Ausübung ihrer Rechte zu gewährleisten (vgl. zur korrespondierenden Bestimmung der Strafprozeßordnung 1975: *Reindl-Krauskopf* in Fuchs/Ratz, WK StPO § 139 [Stand 1.11.2019, rdb.at], Rz. 8).

### III. Legistische und sprachliche Bemerkungen

#### **Zum Titel:**

Der Titel der Novelle sollte unter korrekter Verwendung des Kurztitels der zu ändernden Rechtsvorschrift bezeichnet werden. Er sollte daher „Bundesgesetz, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz geändert wird“ lauten (LRL 120).

Dies gilt auch für den Einleitungssatz.

#### **Zum Inhaltsverzeichnis:**

Es wird angeregt, dem Gesetz ein Inhaltsverzeichnis voranzustellen (LRL 119). Diesfalls wäre das Inhaltsverzeichnis auch in der Inkrafttretensbestimmung (vgl. Z 15) zu nennen.

#### **Zu Z 2 (6 Abs. 3):**

Bei der Zitierung einzelner Bestimmungen einer anderen Rechtsvorschrift ist vor deren Kurztitel der bestimmte Artikel zu verwenden (vgl. LRL 136). Auf die korrekte Bezeichnung des Kurztitels ist zu achten. Es müsste daher „§ 11 des Sanktionengesetzes 2010 – SanktG, BGBl. I Nr. 36/2010, nach § 50 Abs. 1a des Waffengesetzes 1996 – WaffG, BGBl. I Nr. 12/1997, [...]“ lauten.

#### **Zu Z 3 und 4 (§ 6 Abs. 4 und 5):**

Die Novellierungsanordnungen zu Z 3 und 4 könnten zu einer Novellierungsanordnung zusammengefasst werden und wie folgt lauten:

*„3. § 6 Abs. 4 wird durch folgende Abs. 4 und 5 ersetzt:“*

Im geplanten § 6 Abs. 4 wird unter Z 2 auf eine Norm der Strafprozeßordnung 1975 – StPO, BGBl. Nr. 631/1975, verwiesen. Da es sich dabei um die erste Zitierung einer Bestimmung dieses Gesetzes im Staatsschutz- und Nachrichtendienst-Gesetz handelt, sollte es mit seinem Kurztitel, der Abkürzung und der Fundstelle zitiert werden. In der Folge kann die

Abkürzung verwendet werden. In diesem Sinne sollte der Verweis auf § 157 Abs. 1 Z 2 bis 4 StPO in § 9 SNG angepasst werden.

**Zu Z 5 (§ 9 Abs. 2a):**

Die Novellierungsanordnung könnte – kürzer – auch wie folgt formuliert werden:

*„Nach § 9 Abs. 2 wird folgender Abs. 2a eingefügt:“*

**Zu Z 6, 7 und 8 (§ 11):**

Zur Novellierungsanordnung:

Es wird angeregt, die Novellierungsanordnungen Z 6, 7 und 8 wie folgt zusammenzufassen:

*„§ 11 lautet:“*

Diesfalls hätte in Z 15 (§ 18 Abs. 9) die Anordnung des Außerkrafttretens des § 11 Abs. 1a zu entfallen.

Zu Abs. 1:

In Z 5 ist bei der Zitierung des Kurztitels jeweils der bestimmte Artikel zu ergänzen (vgl. die Ausführungen zu Z 2). Es sollte daher im zweiten Klammerausdruck „§ 160 Abs. 3 Z 1 des Telekommunikationsgesetzes 2021 – TKG 2021, BGBl. I Nr. 190/2021“ und im dritten Klammerausdruck „§ 3 Z 2 des E-Commerce-Gesetzes – ECG, BGBl. I Nr. 152/2001“ lauten.

**Zu Z 9 (§ 14 Abs. 2):**

Dem anzufügenden Satz sollte die richtige Formatvorlage („23\_Satz\_(nach\_Novao)“) zugeordnet werden.

**Zu Z 10 (§ 14 Abs. 4):**

In Abs. 4 sollte die „Direktion Staatsschutz- und Nachrichtendienst“ mit die „Direktion“ abgekürzt werden (vgl. § 1 Abs. 3 SNG).

Es wird darauf hingewiesen, dass der Ausdruck „binnen drei Tagen“ alle Wochentage, daher auch Samstage, Sonntage und gesetzliche Feiertage umfasst. Sofern nur Werktage gemeint sein sollten, wäre dies ausdrücklich zum Ausdruck zu bringen.

**Zu Z 12 (§ 15a samt Überschrift):**Abs. 1:

Die „Direktion Staatsschutz- und Nachrichtendienst“ sollte mit „Direktion“ abgekürzt werden (vgl. die Anmerkung zu Z 10).

Abs. 1 sollte sprachlich überarbeitet werden. Nach dem vorgesehenen Wortlaut ist Voraussetzung für die Vornahme der Ermittlungsmaßnahme lediglich die Stellung eines Antrags auf Bewilligung an das Bundesverwaltungsgericht. Es sollte unmissverständlich zum Ausdruck gebracht werden, dass eine Ermittlungsmaßnahme gemäß § 11 Abs. 1 Z 8 und 9 nur aufgrund einer vorab einzuholenden gerichtlichen Bewilligung erfolgen darf.

Abs. 3:

Die „Direktion Staatsschutz- und Nachrichtendienst“ sollte mit „Direktion“ abgekürzt werden (vgl. die Anmerkung zu Z 10).

Das Zitat in Abs. 3 hat richtigerweise „§ 20 des Bundesverwaltungsgerichtsgesetzes – BVwGG, BGBl. I Nr. 10/2013,“ zu lauten (vgl. die Anmerkung zu Z 2).

Abs. 8:

Die Formulierung „Sicherheitsbehörde oder Staatsanwaltschaft“ in Z 2 ist missverständlich, zumal keine Wahlmöglichkeit hinsichtlich der Verständigungspflicht besteht (vgl. auch die Erläuterungen). Es sollte besser „Sicherheitsbehörde bzw. Staatsanwaltschaft“ lauten. Der Verweis auf § 100 StPO sollte zudem präzisiert werden.

**Zu Z 13 (§ 16 Abs. 2 und 3):**

Es wird auf einen Fehler in der Novellierungsanordnung aufmerksam gemacht („lautet“ statt „lauten“):

„§ 16 Abs. 2 und 3 lautet:“

**Zu Z 14 (§ 17 Abs. 3):**

Folgende Novellierungsanordnung wird vorgeschlagen:



„In § 17 Abs. 3 wird nach der Wortfolge „nach § 8 Abs. 2 erster Satz“ die Wortfolge „... die Durchführung von Ermittlungsmaßnahmen nach § 11 Abs. 1 Z 8 oder 9“ eingefügt.“

#### **Zu Z 15 (§ 18 Abs. 9):**

Zu dem in Abs. 9 verwendeten Platzhalter „xx/20xx“ für die BGBl.-Nummer wird darauf aufmerksam gemacht, dass dieser zur leichteren Auffindbarkeit für die Ersetzung im E-Recht einheitlich „xxx/20xx“ lauten sollte.

### **IV. Zu den Materialien**

#### **Zum Vorblatt und zur wirkungsorientierten Folgenabschätzung:**

Dem Regelungsvorhaben wurde keine wirkungsorientierte Folgenabschätzung angeschlossen (siehe zur verpflichtenden Vorlage einer solchen: § 17 Abs. 2 des Bundeshaushaltsgesetzes 2013 – BHG 2013, BGBl. I Nr. 139/2009). Es fehlt somit auch das den Materialien voranzustellende Vorblatt. Eine entsprechende Ergänzung der Gesetzesmaterialien sollte vorgenommen werden.

#### **Zum Allgemeinen Teil der Erläuterungen:**

Im Allgemeinen Teil der Erläuterungen ist – unter „Besonderheiten des Normerzeugungsverfahrens“ – ausdrücklich darauf hinzuweisen, dass der Entwurf nur mit Zustimmung der Länder kundgemacht werden darf (Punkt 94 der Legistischen Richtlinien 1979; siehe dazu oben Pkt. II Zu Z 2).

Es sollte in den Erläuterungen (sowohl im Allgemeinen als auch im Besonderen Teil) auf die korrekte (und einheitliche) Zitierung von Rechtsvorschriften geachtet werden. Im Entwurf werden Rechtsvorschriften teilweise mit ihrem Kurztitel, teilweise nur mit der Abkürzung zitiert. Nur vereinzelt wird die Fundstelle der Rechtsvorschrift genannt. Darüber hinaus sollte darauf geachtet werden, dass die korrekte Abkürzung einer Rechtsvorschrift verwendet wird (etwa „TKG 2021“ statt „TKG“). Vor diesem Hintergrund wird eine Überarbeitung der Materialien empfohlen.

Es sollte auf die durchgehende Verwendung geschützter Leerzeichen geachtet werden (etwa nach „Art.“ oder im Rahmen von Datumsangaben, bzw. bei der Zitierung von Geschäftszahlen von Entscheidungen etc.; (vgl. Layout-Richtlinien 2.1.3).

Im dritten Absatz des Allgemeinen Teils ist ein überflüssiger Beistrich nach „gesetzlich klar definierten“ zu entfernen.

## **Zum Besonderen Teil der Erläuterungen:**

### Allgemeines:

Die Überschriften im Besonderen Teil der Erläuterungen haben dem Muster „Zu Z 1 (§ 6 Abs. 3 Z 3):“ zu folgen (Punkt 93 der Legistischen Richtlinien 1979).

### Zu § 9 Abs. 2a:

Die Anführung jener Fassung, mit der Abs. 1a in § 11 SNG eingefügt wurde (BGBl. I Nr. 148/2021) erscheint überflüssig und kann unterbleiben. Im Übrigen hätte es „idF des Bundesgesetzes BGBl. I Nr. 148/2021“ zu lauten.

### Zu § 11 Abs. 1 Z 8 und 9 sowie Abs. 2 und 3:

Im Zweiten Absatz sollte im ersten Satz nach dem Ausdruck „gesetzlich klar definierten“ der Beistrich entfallen.

Bei der Zitierung von Richtlinien sollte die Fundstelle angegeben werden (vgl. EU-Addendum 54 bis 56).

Zudem wird auf einen Schreibfehler im vierten Absatz aufmerksam gemacht („vergangenen“ statt „vergangen“).

### Zu § 14 Abs. 4 und 5, 15 Abs. 2, 15a sowie 16 Abs. 2:

Im achten Absatz hat es im vorletzten Satz grammatikalisch korrekt „[...] in ihren Rechten verletzt erachten.“ zu lauten. Der verwiesene Art. 133 Abs. 6 Z 1 B-VG normiert die Revision gegen Erkenntnisse des Bundesverwaltungsgerichts. Da es sich bei der vorgesehenen Bewilligung um einen Beschluss handelt, wäre (auch) auf Art. 133 Abs. 9 B-VG zu verweisen.

Im neunten Absatz wird auf ein Schreibversehen aufmerksam gemacht („inklusive“ statt „inklusive“).

Diese Stellungnahme wird im Sinne der Entschlieung des Nationalrates vom 6. Juli 1961 auch dem Prsidium des Nationalrates zur Kenntnis gebracht.

Wien, am 25. September 2024

Fr die Bundesministerin fr EU und Verfassung:

Dr. Albert Posch, LL.M.

Elektronisch gefertigt