Erläuterungen

Allgemeiner Teil

1. Hauptgesichtspunkte des Entwurfs:

Mit dieser Novelle soll einerseits für den Aufgabenbereich des Verfassungsschutzes eine gesonderte Möglichkeit des Aufschubs sicherheitspolizeilichen Einschreitens oder kriminalpolizeilicher Ermittlungen geschaffen werden. Entsprechend der maßgeblichen Bestimmungen in § 23 SPG sowie § 99 Abs. 4 f. StPO soll es den Organisationseinheiten gemäß § 1 Abs. 3 künftig möglich sein, unter Einhaltung sämtlicher dort bereits genannter Voraussetzungen, sicherheitspolizeiliches Einschreiten oder kriminalpolizeiliche Ermittlungen aufzuschieben, soweit ein überwiegendes Interesse an der Erfüllung der Aufgabe nach § 6 Abs. 1 oder 2 besteht.

Andererseits hat die Praxis seit Inkrafttreten des SNG gezeigt, dass die strikte Aufgabenzuweisung der erweiterten Gefahrenerforschung zur Beobachtung einer Gruppierung (§ 6 Abs. 1) zu der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen durch Einzelpersonen (§ 6 Abs. 2) zu den für den Aufgabenbereich Staatsschutz zuständigen Organisationseinheiten (§ 1 Abs. 3) trotz Einrichtung einer Informationsschnittstelle eine rasche, zweckmäßige und effiziente Aufgabenerfüllung in gewissen Fallkonstellationen erschweren kann, weshalb eine Rechtsgrundlage geschaffen werden soll, damit der Direktor im Einzelfall unter gesetzlich festgelegten Kriterien den Aufgabenbereich Nachrichtendienst zu der Wahrnehmung einer Aufgabe nach § 6 Abs. 2 ermächtigen kann.

Weiters soll eine Rechtsgrundlage im SNG geschaffen werden, um in bestimmten, gesetzlich klar definierten, Fällen die Überwachung von Inhaltsdaten nach dem Vorbild der Regelungen in der StPO zu ermöglichen. Angesichts der – insbesondere im Bereich grenzüberschreitender terroristischer Aktivitäten – erfolgten zunehmenden Verlagerung herkömmlicher, unverschlüsselter Telekommunikation auf internetbasierte, zumeist end-to-end-verschlüsselte Kommunikation (wie etwa über WhatsApp, Skype oder Signal) soll zusätzlich eine Rechtsgrundlage für die Überwachung verschlüsselter Nachrichten zur effektiven Bekämpfung verfassungsschutzrelevanter Bedrohungslagen geschaffen werden.

Schließlich handelt es sich um Ergänzungen des Deliktskatalogs der verfassungsgefährdenden Angriffe um für den Verfassungsschutz relevante Tatbestände des Strafgesetzbuches und des Waffengesetzes sowie um eine redaktionelle Verschiebung.

2. Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich auf Art. 10 Abs. 1 Z 6 („Strafrechtswesen“) und Z 7 („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“) des Bundes-Verfassungsgesetzes – B-VG, BGBl. Nr. 1/1930.

Besonderer Teil

Zu § 6 Abs. 3 Z 3 und 4:

Es handelt sich um Ergänzungen des Deliktskatalogs der Z 3 und 4 um die für den Verfassungsschutz relevanten Tatbestände des Strafgesetzbuches „Religiös motivierte extremistische Verbindung“ in § 247b StGB und „Überlieferung an eine ausländische Macht“ in § 103 StGB sowie um die Qualifikation des § 50 Abs. 1a Waffengesetz, welcher insbesondere den illegalen Waffenhandel unter Strafe stellt.

Zu § 6 Abs. 4:

Bislang sah § 6 Abs. 4 nur die Möglichkeit eines besonderen Aufschubs kriminalpolizeilicher Berichtspflichten im Bereich des Verfassungsschutzes vor. Nicht geregelt war jedoch, wie bei Zusammentreffen einer Aufgabe nach § 6 Abs. 1 oder 2 mit (sonstigen) sicherheits- oder kriminalpolizeilichen Aufgaben vorzugehen ist. Die bestehenden Regelungen zum Aufschub sicherheitspolizeilichen Einschreitens nach § 23 SPG oder kriminalpolizeilicher Ermittlungen nach § 99 Abs. 4 StPO berücksichtigen die relevanten Aufgaben des Verfassungsschutzes nicht und erschweren damit eine effiziente Bekämpfung verfassungsgefährdender Strukturen. Aus diesem Grund soll § 6 Abs. 4 eine Überarbeitung erfahren, um auch hinsichtlich der Aufgaben des Verfassungsschutzes einen Aufschub sicherheitspolizeilichen Einschreitens oder kriminalpolizeilicher Ermittlungen zu ermöglichen. Entsprechend der maßgeblichen Bestimmungen in § 23 SPG sowie § 99 Abs. 4 f StPO soll es den Organisationseinheiten gemäß § 1 Abs. 3 künftig möglich sein, unter Einhaltung sämtlicher dort bereits genannter Voraussetzungen, sicherheitspolizeiliches Einschreiten oder kriminalpolizeiliche Ermittlungen

aufzuschieben, soweit ein überwiegendes Interesse an der Erfüllung der Aufgabe nach § 6 Abs. 1 oder 2 besteht; das Interesse an der Aufgabenerfüllung nach § 6 Abs. 1 oder 2 muss dabei eindeutig und offenkundig überwiegen (vgl. *Pilnacek*/*Pleischl* in *Fuchs*/*Ratz*, WK StPO, Vorverfahren § 99 Rz 402). Es kommt immer auf die Abwägung und Beurteilung im Einzelfall an (vgl. *Vogl* in *Fuchs*/*Ratz*, WK StPO § 99 Rz 13).

Das sicherheitspolizeiliche Einschreiten darf darüber hinaus nur aufgeschoben werden, solange keine Gefahr für Leben und Gesundheit Dritter besteht und dafür Vorsorge getroffen ist, dass ein aus der Tat entstehender Schaden zur Gänze gutgemacht wird (§ 23 Abs. 2 SPG). Ein Aufschub kriminalpolizeilicher Ermittlungen setzt zusätzlich voraus, dass – bei gebotener ex-ante Betrachtung – mit dem Aufschub keine ernste Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit Dritter verbunden ist (§ 99 Abs. 4 StPO). Die Befugnis zum Aufschub kriminalpolizeilicher Ermittlungen steht der Kriminalpolizei grundsätzlich aus eigenem zu. Die Staatsanwaltschaft ist von einem solchen Aufschub allerdings unverzüglich zu verständigen (§ 99 Abs. 5 StPO), weil mit dem Aufschub zumindest ein vorläufiger Verzicht auf die Strafverfolgung verbunden sein kann (vgl. EBRV StPRG 131; *Pilnacek*/*Pleischl* in *Fuchs*/*Ratz*, WK StPO, Vorverfahren § 99 Rz 404). Auf Grund ihrer Leitungsfunktion kann die Staatsanwaltschaft, falls sie es für erforderlich hält und nicht ohnehin Einvernehmen über das weitere Vorgehen erzielt werden kann, die Anordnung treffen, den Aufschub zu beenden und die kriminalpolizeilichen Ermittlungen fortzusetzen (*Vogl* in *Fuchs*/*Ratz*, WK StPO § 99 Rz 15).

Die Gründe für den Aufschub sicherheitspolizeilichen Einschreitens oder kriminalpolizeilicher Ermittlungen sind zu dokumentieren.

Zu § 6 Abs. 5:

Gemäß der strikten Aufgabenzuweisung in § 1 Abs. 4 obliegt die Aufgabe der erweiterten Gefahrenerforschung zur Beobachtung einer Gruppierung (§ 6 Abs. 1) der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion und der vorbeugende Schutz vor verfassungsgefährdenden Angriffen durch Einzelpersonen (§ 6 Abs. 2) den für den Aufgabenbereich Staatsschutz zuständigen Organisationseinheiten (§ 1 Abs. 3). Zur Koordinierung dieser beiden Aufgabenbereiche ist innerhalb der Direktion eine Informationsschnittstelle eingerichtet, welcher insbesondere der tagesaktuelle und anlassbezogene Informations- und Lageaustausch, die Bewertung von Informationen sowie die Abstimmung strategischer und operativer Maßnahmen obliegt (§ 2 Abs. 1).

Allerdings hat die Praxis seit Inkrafttreten des SNG gezeigt, dass diese strikte Aufgabenzuweisung trotz Einrichtung der Informationsschnittstelle eine rasche, zweckmäßige und effiziente Aufgabenerfüllung in gewissen Fallkonstellationen erschweren kann (vgl. auch *Salimi*, Gefährliche Gruppierungen, Rz. 60), weshalb der Direktor im Einzelfall unter gesetzlich festgelegten Kriterien den Aufgabenbereich Nachrichtendienst mit der Wahrnehmung einer Aufgabe nach § 6 Abs. 2 ermächtigen dürfen soll.

Um eine Ermächtigung nach Z 1 erteilen zu können, muss durch den Aufgabenbereich Nachrichtendienst bereits eine Aufgabe der erweiterten Gefahrenerforschung wahrgenommen werden, im Zuge derer sich für eine Einzelperson – aus der Gruppierung gemäß § 6 Abs. 1 – auch die Voraussetzungen des § 6 Abs. 2 ergeben. Wenn eine Übergabe dieser sich neu stellenden Aufgabe gemäß § 6 Abs. 2 an den Aufgabenbereich Staatsschutz im konkreten Anlassfall die Aufgabenerfüllung etwa aufgrund besonderer Dringlichkeit beeinträchtigen oder zu Doppelgleisigkeiten der Ermittlungen führen würde, kann der Direktor im Einzelfall von dieser Ermächtigung Gebrauch machen.

Die Erteilung einer Ermächtigung gemäß Z 2 ist dann zulässig, wenn dem Aufgabenbereich Nachrichtendienst Informationen von Dienststellen inländischer Behörden, ausländischen Sicherheitsbehörden oder Sicherheitsorganisationen übermittelt werden, die eine Aufgabe nach § 6 Abs. 2 begründen, die genannten Informationen aber einer Verarbeitungsbeschränkung unterliegen, sodass diese nach den Vorgaben der übermittelnden Stelle nur von mit nachrichtendienstlichen Aufgaben betrauten Organisationseinheiten verarbeitet werden dürfen. Die Verarbeitungsbeschränkung kann sich unmittelbar aus § 9 PolKG ergeben, aber auch aus vergleichbaren nationalen, internationalen oder bilateralen Verpflichtungen. Die Informationen können sowohl von ausländischen oder internationalen übermittelnden Stellen (zB. ausländische Partnerdienste) als auch von inländischen Behörden (etwa Heeres-Nachrichtenamt oder Abwehramt) stammen.

Voraussetzung für jede Erteilung einer Ermächtigung gemäß Z 1 oder 2 ist es überdies, dass die Wahrnehmung der Aufgabe nach § 6 Abs. 2 durch den Aufgabenbereich Nachrichtendienst im jeweiligen Fall im Interesse der Raschheit und Zweckmäßigkeit geboten ist (vgl. auch § 14 Abs. 3 SPG).

Wird eine entsprechende Ermächtigung erteilt, ist seitens der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit nach den herkömmlichen Regelungen des SNG vorzugehen und

insbesondere die Ermächtigung des Rechtsschutzbeauftragten für die konkrete Aufgabe nach § 6 Abs. 2 einzuholen (vgl. § 14).

Jede Aufgabenübertragung gemäß Abs. 5 bedarf einer eigenen Ermächtigung des Direktors. Der Direktor hat den Leiter der Informationsschnittstelle (§ 2 Abs. 1) sogleich bei Beginn und Ende jeder Aufgabenwahrnehmung zu informieren, insbesondere damit dieser die allenfalls erforderlichen Abstimmungen strategischer und operativer Maßnahmen wahrnehmen kann.

Zu § 9 Abs. 2a:

Es handelt sich um eine – im Wesentlichen – redaktionelle Verschiebung des § 11 Abs. 1a idF BGBl. I Nr. 148/2021 zur Klarstellung, dass sich die bereits in § 11 Abs. 1a idF BGBl. I Nr. 148/2021 vorgesehene Regelung grundsätzlich auf die Verarbeitung von personenbezogenen Daten im Aufgabenbereich Nachrichtendienst bezieht.

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

Bislang ermöglicht das SNG den Verfassungsschutzbehörden im Hinblick auf Telekommunikation lediglich die Ermittlung von Verkehrsdaten, Kommunikationsinhaltsdaten können dahingegen nicht ermittelt werden. Praktische Erfahrungen im Zusammenhang mit dem vorbeugenden Schutz vor verfassungsgefährdenden Angriffen – insbesondere im Hinblick auf die Abwehr geplanter terroristischer Anschläge – sowie der internationale Vergleich haben allerdings gezeigt, dass das Fehlen einer Möglichkeit zur effizienten Überwachung des Kommunikationsverkehrs die Aufgabenerfüllung der Verfassungsschutzbehörden erheblich erschwert. So steht etwa in Deutschland die Überwachung der Inhalte sowohl von konventioneller wie auch verschlüsselter Kommunikation nicht nur den Strafverfolgungsbehörden, sondern auch den Sicherheitsbehörden und Nachrichtendiensten zur Verfügung. Da ohne die Überwachung von Inhaltsdaten keine konkreten Hinweise auf bevorstehende verfassungsgefährdende Angriffe – etwa hinsichtlich potentieller (Mit-)Täter, Art und Weise des drohenden Angriffs, Begehungsorte oder -zeitpunkte – gewonnen werden können, sind die österreichischen Verfassungsschutzbehörden, mangels Substituierbarkeit der Inhaltsüberwachung durch bestehende Ermittlungsmaßnahmen, in vielen Fällen auf Informationen von Partnerdiensten angewiesen, die mitunter aufgrund ihrer Klassifizierung nur eingeschränkt für Strafverfolgungszwecke verwendet werden können.

Aus diesen Gründen sollen nunmehr die Rechtsgrundlagen im SNG geschaffen werden, um in bestimmten, gesetzlich klar definierten, Fällen die Überwachung von Inhaltsdaten nach dem Vorbild der Regelungen in der StPO zu ermöglichen. Angesichts der – insbesondere im Bereich grenzüberschreitender terroristischer Aktivitäten – erfolgten zunehmenden Verlagerung herkömmlicher, unverschlüsselter Telekommunikation auf internetbasierte, zumeist end-to-end-verschlüsselte Kommunikation (wie etwa über WhatsApp, Skype oder Signal) soll zusätzlich auch eine Rechtsgrundlage für die Überwachung verschlüsselter Nachrichten zur effektiven Bekämpfung von verfassungsschutzrelevanten Bedrohungslagen geschaffen werden. In diesem Sinne betont auch die Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung die Bedeutung der Zurverfügungstellung wirksamer Ermittlungsinstrumente, wie insbesondere der Überwachung des Kommunikationsverkehrs, für die Bekämpfung terroristischer Straftaten (Art. 20 sowie Erwägungsgrund 21 der Terrorismus-RL). In dem rezenten Erkenntnis des VfGH zur Sicherstellung und Auswertung von Datenträgern trägt das Höchstgericht ebenso dem Umstand Rechnung, dass „*staatliches Handeln durch die rasche Verbreitung der Nutzung neuer Kommunikationstechnologien in vielerlei Hinsicht vor besondere Herausforderungen gestellt wurde und wird.*“ Dieses geänderte Umfeld ist nach der Rechtsprechung des VfGH auch maßgeblich bei der Beurteilung der Befugnisse zu berücksichtigen (VfGH vom 14. Dezember 2023, G 352/2021 Rn 2.2.8.).

In Anbetracht dieser Erwägungen und unter Berücksichtigung jener Argumentationslinien, die den Verfassungsgerichtshof mit Erkenntnis vom 11. Dezember 2019, G 72-74/2019, G 181-182/2019, zur Aufhebung der strafprozessualen Ermittlungsmaßnahme der „Überwachung verschlüsselter Nachrichten“ gemäß § 135a StPO idF BGBl. I Nr. 27/2018 veranlasst haben, soll zur Vorbeugung bestimmter, besonders schwerwiegender verfassungsgefährdender Angriffe durch die Einführung von § 11 Abs. 1 Z 8 und 9 die Überwachung sowohl unverschlüsselter als auch verschlüsselter Nachrichten im Rahmen dieses Gesetzes ermöglicht werden. Der im zitierten Erkenntnis geäußerten Ansicht des VfGH, eine derartige verdeckte Überwachung verschlüsselter Nachrichten dürfe nur in Bezug auf Straftaten erfolgen, die im Einzelfall eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darstellen und die einen solchen schwerwiegenden Eingriff rechtfertigen (vgl. Rn. 190), wird durch folgende Vorkehrungen Rechnung getragen:

Bereits durch die Verortung gegenständlicher Ermittlungsmaßnahmen im SNG wird eine Beschränkung ihres Anwendungsbereichs auf die Zwecke des Verfassungsschutzes erzielt. Dabei soll die Überwachung

sowohl von unverschlüsselten als auch verschlüsselten Nachrichten auf die Vorbeugung gesetzlich determinierter, besonders schwerwiegender verfassungsgefährdender Angriffe durch eine Person beschränkt sein. Unter derartigen Angriffen sind ausschließlich verfassungsgefährdende Angriffe, die im Falle ihrer Verwirklichung zumindest mit bis zu zehn Jahren Freiheitsstrafe bedroht wären oder den Tatbestand des § 256 StGB erfüllten, zu verstehen. Die Aufnahme des Tatbestandes des § 256 StGB ist vor dem Hintergrund der geopolitischen Entwicklungen – etwa dem Angriffskrieg Russlands auf die Ukraine – besonders bedeutend. In den vergangen zwei Jahren konnte eine Zunahme von Spionageaktivitäten in Österreich festgestellt werden. Überdies können Spionageaktivitäten auch transnationale Repressionen – insbesondere politische Verfolgung, die von autoritären Staaten außerhalb ihres Staatsgebietes ausgeübt wird – zum Ziel haben, womit eine Gefahr für Leib, Leben und Freiheit der Betroffenen verbunden sein kann.

Durch den Verweis auf die Legaldefinition der „Überwachung von Nachrichten“ in § 134 Z 3 StPO soll für die neuen Ermittlungsmaßnahmen unmittelbar an die für den strafprozessualen Bereich bereits etablierte Begriffsbestimmung und -abgrenzung angeknüpft werden. Gegenstand der Überwachung nach Z 8 und 9 dürfen demnach lediglich von einer natürlichen Person über ein Kommunikationsnetz (§ 4 Z 1 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) (unverschlüsselt oder verschlüsselt) gesendete, übermittelte oder empfangene Nachrichten und Informationen sowie mit dem Übertragungsvorgang unmittelbar in Zusammenhang stehende Stamm-, Zugangs- und Verkehrsdaten sein. Eine Online-Durchsuchung des gesamten Computersystems inklusive lokal abgespeicherter Daten ist sowohl aufgrund der ausdrücklichen Eingrenzung auf Nachrichten, die mit einem Übertragungsvorgang in Zusammenhang stehen, als auch der in § 15a Abs. 3 festgelegten Beschränkung der gerichtlichen Bewilligung der Maßnahme auf jenen künftigen Zeitraum, der zur Erfüllung der Aufgabe nach § 6 Abs. 2 voraussichtlich erforderlich ist, nicht zulässig. In diesem Sinne ist auch im Rahmen der Durchführung einer Ermittlungsmaßnahme nach Z 9 gemäß § 15a Abs. 5 Z 1 technisch sicherzustellen, dass von der eingesetzten Software ausschließlich innerhalb des seitens des Bundesverwaltungsgerichts festgelegten Bewilligungszeitraums gesendete, übermittelte oder empfangene Nachrichten überwacht werden können.

Von der Überwachung erfasst sind daher 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, zumal auch hier eine Übermittlung an einen anderen Server stattfindet. Durch das ausdrückliche Abstellen auf einen Übertragungsvorgang ist hingegen die Überwachung von lokal gespeicherten Daten sowie die autonome Kommunikation zweier Endgeräte mangels erforderlichen menschlichen Zutuns (M2M-Kommunikation) nicht umfasst.

Hinsichtlich der technischen Durchführung der Überwachung unverschlüsselt kommunizierter Nachrichten gemäß Z 8 kann auf die im Rahmen des Vollzugs der Ermittlungsmaßnahme nach § 134 Z 3 StPO gesammelten Erfahrungswerte und die hierfür geschaffenen technischen Strukturen zurückgegriffen werden. Die Ausleitung der im Rahmen der Kommunikationsverbindung bei dem Betreiber des verwendeten Kommunikationsnetzes oder sonstigen Dienstes der Informationsgesellschaft anfallenden Nachrichten und Informationen erfordert bei unverschlüsselten Nachrichten keinen zusätzlichen Eingriff in das Kommunikationsmedium der zu überwachenden Person. Für die Überwachung verschlüsselter Datenströme gemäß Z 9 bedarf es dahingegen zusätzlich des Einbringens eines Programmes in das betreffende Computersystem, um end-to-end verschlüsselt gesendete, übermittelte oder empfangene Nachrichten und Informationen noch vor deren Verschlüsselung bzw. nach deren Entschlüsselung ermitteln zu können. Durch das Programm werden somit lediglich jene Kommunikationsinhalte und damit in Zusammenhang stehende Daten lesbar gemacht, die auch bisher schon im Rahmen einer Überwachung von Nachrichten nach § 134 Z 3 StPO ermittelt werden können. Unter „Computersystem“ im Sinne des § 74 Abs. 1 Z 8 StGB sind sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen, zu subsumieren. Die Ermittlungsmaßnahmen erfassen somit nicht nur den klassischen Computerbegriff, sondern auch andere Geräte, die eine Internetverbindung ermöglichen, wie insbesondere Smartphones und Tablets. Durch den Verweis auf die Definition des StGB soll insbesondere die Schaffung verwechslungsanfälliger neuer Terminologien vermieden werden.

Bei dem zur Überwindung der Transportverschlüsselung einzubringenden Programm handelt es sich um eine Software, die Nachrichten und Informationen noch vor deren Verschlüsselung bzw. nach der Entschlüsselung im Rahmen der Vorgänge des Sendens, Übermittelns und Empfangens ausleiten kann. Vor ihrer Einbringung ist die Software individuell auf das zu überwachende Computersystem – insbesondere unter dem Gesichtspunkt, die Überwachung auf das zur Erfüllung der Aufgabe unbedingt erforderliche Ausmaß zu beschränken und die Einhaltung der Beschränkungen des § 15a Abs. 5

sicherzustellen – abzustimmen. Zu diesem Zweck ist vorab insbesondere eine Eingrenzung der Zugriffsmöglichkeiten der Software auf bestimmte Kommunikationsapplikationen zu prüfen. Zur anschließenden Einbringung des Programms ohne Kenntnisnahme des Betroffenen dürfen technische Mittel eingesetzt werden. Im Rahmen einer remote-Einbringung, bei der kein physischer Zugriff auf das zu überwachende Gerät stattfindet, kommt insbesondere der eindeutigen Zuordnung des Zielcomputersystems zum Betroffenen vor und während der Maßnahme, beispielsweise durch entsprechende begleitende Ermittlungsmaßnahmen wie Observation oder eindeutige Identifikation durch Mac-Adresse, Seriennummer, Geräte-ID, IMSI- oder IMEI-Nummer oder individuelle IP-Adresse, besondere Bedeutung zu. Die einzubringende Software ist technisch regulierbar, sodass nur gezielte und von der Bewilligung umfasste Nachrichten aus bestimmten Applikationen ausgeleitet werden können. Zum Zweck der Eruierung dieser Identifikationsdaten wird dem Einsatz einer Ermittlungsmaßnahme nach Z 8 oder 9 regelmäßig die Ermittlung personenbezogener Daten insbesondere durch Observation und Anfrage an Betreiber öffentlicher Telekommunikationsdienste und sonstige Diensteanbieter nach Maßgabe der Z 5 und 7 vorangehen. Ein Eindringen in vom Hausrecht geschützte Räume oder Durchsuchen von Behältnissen zwecks Installation des Programms ist nicht zulässig.

Die Überwachung konventioneller wie auch verschlüsselt kommunizierter Nachrichten ist überdies nur zulässig, wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. Indem das Erfordernis der Aussichtslosigkeit anderer Ermittlungsmaßnahmen nunmehr alleinig für die neuen Befugnisse der Überwachung von (unverschlüsselten und verschlüsselten) Nachrichten ausdrücklich angeordnet wird, soll der Sonderstellung und spezifischen Eingriffsintensität dieser verdeckten Maßnahmen Rechnung getragen werden. Die Zulässigkeit der Überwachung von Nachrichten gemäß Z 8 zur Durchführung einer Maßnahme nach Z 9 stellt insofern eine notwendige Einschränkung des ultima-ratio-Erfordernisses dar, als die Überwachung nach Z 8 für die Eruierung, welche Kommunikationskanäle der Betroffene nutzt, und somit die treffsichere Einbringung des Programms zur Überwachung verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten erforderlich ist. Die Maßnahme nach Z 8 muss somit auch in Fällen einsetzbar sein, in denen sie selbst hinsichtlich der Inhaltsüberwachung von Nachrichten zwar nicht erfolgsversprechend erscheint, weil beispielsweise durch (verdeckte) Observation bereits festgestellt werden konnte, dass der Betroffene ausschließlich verschlüsselt kommuniziert, aber Voraussetzung für die erfolgreiche Überwachung verschlüsselter Nachrichten ist.

Aufgrund der Einführung der neuen Ermittlungsmaßnahmen gemäß Abs. 1 Z 8 und 9 sind auch die Abs. 2 und 3, die die Mitwirkungs- und Verschwiegenheitspflichten der ersuchten Stellen sowie die einschlägigen Kostenersatzbestimmungen enthalten, anzupassen.

Zu § 11 Abs. 1 Z 1, 2, 3, 5 und 7:

Im Zuge der Erarbeitung der Z 8 und 9 hat sich gezeigt, dass die für die bestehenden Ermittlungsbefugnisse des § 11 Abs. 1 normierten ultima-ratio-Vorgaben die ermittlungstaktischen Zusammenhänge der einzelnen Befugnisse, die bisweilen den gleichzeitigen Einsatz mehrerer Ermittlungsmaßnahmen erfordern, nicht adäquat widerspiegeln. Um Unklarheiten bezüglich des Zusammenspiels der Ermittlungsmaßnahmen hintanzuhalten, sollen die Z 1, 2, 3, 5 und 7 entsprechend angepasst werden, sodass – wie auch schon bisher – jeder Befugnisausübung nach § 11 eine Verhältnismäßigkeitsprüfung unter Abwägung der Eingriffsschwere und des angestrebten Erfolges sowie Berücksichtigung der in § 29 SPG festgelegten allgemeinen Grundsätze voranzugehen hat.

Zu § 11 Abs. 1 Z 5 und 7:

Mit der Ergänzung der Ermittlungsmaßnahme nach Z 5 soll eine Anpassung an die korrespondierende Bestimmung der StPO (§ 134 Z 2a StPO) erfolgen, in der mit BGBl. I Nr. 27/2018 eine Legaldefinition zur Lokalisierung einer technischen Einrichtung eingeführt wurde. Durch die Einführung einer Legaldefinition sollte klargestellt werden, dass es sich bei der Lokalisierung einer technischen Einrichtung um den Einsatz technischer Mittel zur Feststellung von geografischen Standorten und der zur internationalen Kennung des Benutzers dienenden Nummer (IMSI) ohne Mitwirkung des Anbieters (oder sonstigen Diensteanbieters) handelt. Diese Klarstellung soll nunmehr auch für den Bereich des Staatsschutzes und Nachrichtendienstes nachgezogen werden.

Mit der gegenständlichen Änderung der Z 7 soll außerdem eine Rechtsgrundlage für den Einsatz von technischen Mitteln, insbesondere WLAN-Catchern, geschaffen werden, mit deren Hilfe die Ermittlung von Verkehrs-, Zugangs und Standortdaten ohne Einbeziehung von Betreibern öffentlicher Telekommunikationsdienste (§ 160 Abs. 3 Z 1 TKG 2021) und sonstigen Diensteanbietern (§ 3 Z 2 ECG) ermöglicht werden soll.

Für den Einsatz technischer Mittel nach Z 5 und Z 7 ist nach den herkömmlichen Regelungen des SNG eine Ermächtigung des Rechtsschutzbeauftragten einzuholen (vgl. § 14).

Zu § 14 Abs. 2:

Die für die Ermächtigung des Rechtsschutzbeauftragten zur Ermittlung personenbezogener Daten nach Z 7 angeordnete Beschränkung auf jenen künftigen oder vergangenen Zeitraum, der zur Erreichung des Zwecks voraussichtlich erforderlich ist, wurde aufgrund systematischer Erwägungen zu den übrigen die Ermächtigung des Rechtsschutzbeauftragten betreffenden Bestimmungen in § 14 Abs. 2 verschoben.

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

In Anbetracht der spezifischen Eingriffsintensität der neuen Ermittlungsmaßnahmen nach § 11 Abs. 1 Z 8 und 9 sowie der technischen Besonderheiten, die mit der Überwachung verschlüsselter Nachrichten verbunden sind, sollen durch die folgenden Anpassungen – insbesondere die Einführung der besonderen Rechtsschutzbestimmungen des § 15a – engmaschig flankierende Regelungen, die den Persönlichkeitsschutz und das Grundrecht auf Datenschutz angemessen würdigen, geschaffen werden. Um einen besonders hohen Schutzstandard zu gewährleisten und dem mit diesen Ermittlungsmaßnahmen erstmals verbundenen Eingriff in das unter Richtervorbehalt stehende Fernmeldegeheimnis gemäß Art. 10a StGG, RGBl. Nr. 142/1867, (die Ermittlung von Verkehrsdaten gemäß § 11 Abs. 1 Z 7 stellt keinen Eingriff in das Fernmeldegeheimnis dar, vgl. auch Pkt. 8.2. des Erkenntnisses des VfGH vom 29. November 2017, G 223/2016) unter formellen Gesichtspunkten entsprechend Rechnung zu tragen, soll im Zuge der Einführung dieser Ermittlungsmaßnahmen ein innerhalb dieses Gesetzes neuartiges Rechtsschutzsystem im Sinne eines mehrstufigen Bewilligungs- und Kontrollverfahrens unter Einbindung des Bundesverwaltungsgerichts (§ 15a) sowie des gemäß § 91a SPG beim Bundesminister für Inneres eingerichteten Rechtsschutzbeauftragten (§ 14 Abs. 4 und 5, § 15a Abs. 3, 4 und 8 sowie § 16) etabliert werden. Die Antragstellung für die Bewilligung und die Durchführung der Maßnahmen obliegt ausschließlich der Direktion Staatsschutz und Nachrichtendienst, um die Einheitlichkeit des Vollzugs und die Qualitätssicherung durch Bündelung des (technischen) Know-Hows zu gewährleisten sowie die begleitende Kontrolle der Maßnahme durch den Rechtsschutzbeauftragten angesichts deren örtlicher Zentralisierung zu erleichtern.

Beabsichtigt die Direktion Staatsschutz und Nachrichtendienst die Durchführung einer Überwachung von (verschlüsselten) Nachrichten, hat sie – noch vor ihrem Antrag auf gerichtliche Bewilligung der Maßnahme – den Rechtsschutzbeauftragten zu befassen (§ 14 Abs. 4). Diesem ist durch Mitteilung jener Informationen, die gemäß § 15a Abs. 2 auch einem Antrag an das BVwG zugrunde zu legen wären, binnen einer Frist von drei Tagen Gelegenheit zur Äußerung zu geben (vgl. auch § 91c Abs. 2 SPG). Mit seiner zustimmenden oder ablehnenden Äußerung kann der Rechtsschutzbeauftragte seine Sicht in den Entscheidungsfindungsprozess der Beantragung einer Nachrichtenüberwachung einbringen. Wenngleich seine Äußerung keine direkte Verbindlichkeit hinsichtlich der Entscheidung über die gerichtliche Antragstellung entfaltet, kommt insbesondere einer ablehnenden Stellungnahme im Regelfall normative Kraft aus ihrer Faktizität zu (vgl. *Vogl* in *Thanner/Vogl,* SPG[2] § 91c Rz 15). Durch dieses vorgeschaltete Äußerungsrecht des Rechtsschutzbeauftragten, anstelle seiner bloßen Einbindung im Rahmen des kommissarischen Rechtsschutzes, wird gewährleistet, dass der Rechtsschutzbeauftragte nicht nur die konkrete Durchführung einer Nachrichtenüberwachung kontrollieren und allenfalls ein Rechtsmittel zugunsten des Betroffenen erheben, sondern bereits Bedenken gegen deren Durchführung vorbringen kann und damit zu einer besonderen Wahrung der Verhältnismäßigkeit beiträgt. Gleichzeitig wird durch die Etablierung eines Vier-Augen-Prinzips ein gewisser Qualitätsstandard hinsichtlich der an das BVwG ergehenden Anträge sichergestellt.

Nach Äußerung des Rechtsschutzbeauftragten oder Ablauf der Drei-Tages-Frist kann die Direktion einen, zumindest die in § 15a Abs. 2 angeführten Informationen enthaltenden, Antrag auf Bewilligung der Maßnahme an das BVwG stellen. Es ist sicherzustellen, dass die mit der Antragstellung und Bewilligung in Zusammenhang stehende Kommunikation zwischen der Direktion Staatsschutz und Nachrichtendienst und dem BVwG im elektronischen Weg über einen sicheren Kommunikationskanal erfolgt, um ein möglichst hohes Datensicherheitsniveau zu gewährleisten. In diesem Sinne hat das BVwG überdies sämtliche mit der Antragstellung und Bewilligung in Zusammenhang stehende Daten getrennt vom sonstigen Aktenbestand zu verwahren und auf geeignete Art und Weise gegen unbefugte Einsichtnahme zu sichern.

Der Antrag hat jedenfalls folgende Bestandteile zu umfassen:

1. den Namen oder sonstige Identifizierungsmerkmale des zu überwachenden Betroffenen nach § 6 Abs. 2, wie etwa Geburtsdatum, Geburtsort, Staatsangehörigkeit oder Wohnanschrift;
2. die nach § 14 Abs. 2 grundsätzlich erforderliche Ermächtigung des Rechtsschutzbeauftragten für die Aufgabe nach § 6 Abs. 2 und den Zeitraum, für den diese Ermächtigung erteilt wurde, sowie eine allfällige Äußerung des Rechtsschutzbeauftragten nach § 14 Abs. 4. Sofern keine Äußerung

des Rechtsschutzbeauftragten vorliegt, muss im Antrag ein Hinweis darauf aufgenommen werden;

3. den befürchteten verfassungsgefährdenden Angriff im Sinne § 11 Abs. 1 Z 8 – somit ein verfassungsgefährdender Angriff nach § 256 StGB oder ein solcher, dessen Verwirklichung zumindest mit bis zu zehn Jahren Freiheitsstrafe bedroht ist – sowie jene Tatsachen, aus denen sich ein begründeter Gefahrenverdacht ergibt;
4. sofern erforderlich die Tatsachen, aus denen sich ergibt, dass die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. Ist eine Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 zur Durchführung einer Überwachung von Nachrichten nach § 11 Abs. 1 Z 9 erforderlich, ist gleichfalls im Antrag ein Hinweis darauf aufzunehmen;
5. die Identifizierungsmerkmale der gemäß § 11 Abs. 1 Z 8 zu überwachenden technischen Einrichtung (etwa Rufnummer, IMSI- oder IMEI-Nummer oder individuelle IP-Adresse) oder des gemäß § 11 Abs. 1 Z 9 zu überwachenden Computersystems. Hinsichtlich des zu überwachenden Computersystems sind jene Parameter zu nennen, die vorab zwecks Einbringung des Programms (beispielsweise durch Einsatz einer Ermittlungsmaßnahme nach § 11 Abs. 1 Z 5 oder 7) in Erfahrung gebracht wurden, wie insbesondere Gerätetyp, Betriebssystem, Mac-Adresse, Seriennummer, Geräte-ID, IMSI- oder IMEI-Nummer oder individuelle IP-Adresse;
6. die begehrte Dauer der Überwachung, wobei diese jedenfalls auf jenen Zeitraum, der für die Erfüllung der Aufgabe unbedingt erforderlich erscheint, längstens jedoch auf drei Monate begrenzt sein sollte (vgl. zur zulässigen Bewilligungsdauer § 15a Abs. 3);
7. die Art der Nachrichtenübertragung (zB. Internet-Kommunikation, E-Mail, Sprachtelefonie, Funk, Fax) sowie
8. bei einer Überwachung gemäß § 11 Abs. 1 Z 9 zusätzlich die beabsichtigte Art des Einsatzes technischer Mittel, deren Einsatz die Einbringung des Programms in das zu überwachende Computersystem ermöglichen soll.

Für die Bewilligung der Ermittlungsmaßnahme ist aufgrund bundesgesetzlicher Anordnung in § 15a Abs. 1 gemäß Art. 131 Abs. 4 Z 2 lit. d B-VG, BGBl. Nr. 1/1930, das Bundesverwaltungsgericht zuständig. Über den Antrag entscheidet der nach der Geschäftsverteilung zuständige Einzelrichter des BVwG (§ 6 BVwGG, BGBl. I Nr. 10/2013) mittels begründetem, eine Belehrung enthaltendem Beschluss (§ 29 Abs. 1 und 2a iVm 31 VwGVG, BGBl. I Nr. 33/2013). Durch diese im Bereich der Sicherheitspolizei neuartige verwaltungsgerichtliche Bewilligung soll eine unabhängige gerichtliche Kontrolle sowie ein verstärkter Rechtsschutz zur Gewährleistung der Verhältnismäßigkeit und des Grundrechtsschutzes, insbesondere des unter Richtervorbehalt stehenden Fernmeldegeheimnisses gemäß Art. 10a StGG, etabliert werden.

Die Bewilligung der Maßnahme durch das BVwG darf nur für jenen künftigen Zeitraum, der zur Erfüllung der Aufgabe voraussichtlich erforderlich ist, höchstens aber für drei Monate erteilt werden (§ 15a Abs. 3). Bei der Festlegung des Bewilligungszeitraums hat das BVwG insbesondere die Schwere des befürchteten verfassungsgefährdenden Angriffs sowie die Bestimmtheit jener Anhaltspunkte, die dessen Befürchtung rechtfertigen, zu erwägen. Verlängerungen der Bewilligung sind zulässig, wobei erneute, im Sinne des § 15a Abs. 2 begründete Anträge erforderlich sind. Der Beschluss ist sowohl der Direktion als auch dem Rechtsschutzbeauftragten zuzustellen, um diesem die ihm nach § 14 Abs. 4 im Rahmen des kommissarischen Rechtsschutzes zukommende Prüfung der Bewilligung sowie die allfällige Erhebung einer Revision zugunsten des Betroffenen nach § 15a Abs. 4 unter den Voraussetzungen des § 25a VwGG, BGBl. Nr. 10/1985, binnen einer Frist von sechs Wochen, zu ermöglichen. Aufgrund des Ausschlusses der Geltung von § 20 BVwGG sind im Zusammenhang mit der Beantragung einer Maßnahme nach § 11 Abs. 1 Z 8 oder 9 ergehende Beschlüsse des BVwG – um dem Interesse an Geheimhaltung der konkreten Durchführungsparameter einer Nachrichtenüberwachung nachzukommen – nicht im Rechtsinformationssystem des Bundes (RIS) zu veröffentlichen.

Dem Rechtsschutzbeauftragten obliegt gemäß § 14 Abs. 5 überdies die begleitende Kontrolle der Durchführung der Nachrichtenüberwachung gemäß § 11 Abs. 1 Z 8 und 9. Im Rahmen dieser Kontrolltätigkeit hat er insbesondere darauf zu achten, dass die Grenzen der Bewilligung in zeitlicher Hinsicht eingehalten werden, mithin keine Nachrichten ermittelt werden, die von der Bewilligung nicht gedeckt sind, und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist. Zur effektiven Ausübung der Kontrolle ist dem Rechtsschutzbeauftragten gemäß § 15 Abs. 1 insbesondere jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren und umfassend Auskunft zu erteilen. Nach Beendigung einer Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 oder 9 ist dem Rechtsschutzbeauftragten in Anlehnung an § 147 Abs. 4 StPO überdies Gelegenheit zu geben, die nach § 15 Abs. 7 weiterverarbeiteten Nachrichten einzusehen und anzuhören sowie die

(teilweise) Löschung von Nachrichten, die etwa entgegen der gerichtlichen Bewilligung oder datenschutzrechtlicher Bestimmungen ermittelt wurden, zu beantragen (siehe § 15a Abs. 9). Durch diese begleitende Kontrolle soll die Wahrung der Rechte des von der Nachrichtenüberwachung Betroffenen zu einem Zeitpunkt, in dem dieser noch keine Kenntnisse von deren Durchführung hat, gewährleistet werden.

Die Information des von der Durchführung einer Überwachung von (verschlüsselten) Nachrichten Betroffenen der Aufgabe nach § 6 Abs. 2 hat nach Maßgabe des § 16 Abs. 2 mit Ablauf der Ermächtigung des Rechtsschutzbeauftragten nachweislich zu erfolgen. Darüber hinaus wird die Informationspflicht, um auch dem Rechtsschutz sonstiger, von der Nachrichtenüberwachung betroffener Dritter ausreichend Rechnung zu tragen, auf jene Personen erstreckt, an die oder von denen Nachrichten gesendet, übermittelt oder empfangen wurden, die aufgrund ihrer Erforderlichkeit für die Aufgabenerfüllung weiterverarbeitet wurden, sofern ihre Identität sich ohne besonderen Verfahrensaufwand, somit lediglich durch leicht durchführbare zusätzliche Erhebungen, feststellen lässt (vgl. zur vergleichbaren strafprozessualen Regelung § 139 Abs. 2 StPO). Ab dem Zeitpunkt der Verständigung beziehungsweise einer allenfalls bereits zuvor erfolgten Kenntnisnahme steht es dem Betroffenen oder sonstigen betroffenen Dritten frei, eine Beschwerde wegen Verletzung der Bestimmungen über den Datenschutz nach § 90 SPG aufgrund einer behaupteten Verletzung seiner Rechte durch Verarbeiten personenbezogener Daten entgegen den Bestimmungen des DSG geltend zu machen. Ebenso kommt diesen das Recht zur Erhebung einer Beschwerde wegen Verletzung subjektiver Rechte nach § 88 Abs. 2 SPG zu, sofern sie sich, insbesondere durch die Modalitäten der Durchführung der Ermittlungsmaßnahme, in seinen Rechten verletzt erachten. Letztlich kann der Betroffene auch unmittelbar auf Art. 133 Abs. 6 Z 1 B-VG gestützt gegen den bewilligenden Beschluss des BVwG Revision an den Verwaltungsgerichtshof nach Maßgabe der §§ 25a ff VwGG erheben.

Neben diesen Rechtsschutzgarantien sind angesichts der mit der Einbringung einer Software zur Überwachung unverschlüsselter Kommunikation nach § 11 Abs. 1 Z 9 verbundenen technischen Besonderheiten dieser Ermittlungsmaßnahme ergänzende Schutzvorkehrungen gemäß § 15a Abs. 5 zu treffen. So ist durch entsprechende Programmierung der Software zu gewährleisten, dass ausschließlich innerhalb des Bewilligungszeitraums gesendete, übermittelte oder empfangene Nachrichten überwacht werden können. Es ist sicherzustellen, dass mit der Durchführung der Überwachung keine über die Installation und die mit der Überwachung notwendig einhergehenden Eingriffe hinausgehenden Veränderungen des zu überwachenden Computersystems inklusiver der auf ihm gespeicherten Daten verbunden sind. Nach Beendigung der Ermittlungsmaßnahme muss sichergestellt sein, dass die eingebrachte Software ohne dauerhafte Beschädigung oder Beeinträchtigung des Computersystems vollständig entfernt oder funktionsunfähig wird. Dies kann in der Praxis durch die Ausgestaltung des Programms mit einem sogenannten „Kill-Switch“ sichergestellt werden, der nach Ablauf der vorgegebenen Frist oder bereits zuvor durch remote-Betätigung (beispielsweise, wenn die Maßnahme vorzeitig zu beenden ist, etwa weil das Gerät weitergegeben wurde und von einer anderen als der Zielperson verwendet wird) die vollständige forensische und sichere Löschung der Überwachungssoftware gewährleistet. Ebenso kann in die Software eine laufende Datumsprüfung eingebaut werden, sodass diese bei Erreichen eines bestimmten Datums automatisch gelöscht wird, unabhängig davon, ob eine Verbindung mit dem Internet besteht.

Um die Authentizität und Integrität der erhobenen Nachrichten sowie die Nachverfolgbarkeit deren Ermittlung zu gewährleisten, sieht § 15a Abs. 6 spezifische Dokumentationspflichten vor. Durch die automationsunterstützte Dokumentation dieser Parameter soll insbesondere sichergestellt werden, dass die Installation des Programms sowie jede sonstige durch die Software an dem Computersystem vorgenommene, nicht bloß flüchtige Veränderung nachvollziehbar bleibt. Die bestehenden Protokollierungspflichten nach § 50 DSG bleiben von diesen erweiterten Dokumentationspflichten unberührt.

Der Bundesminister für Inneres ist datenschutzrechtlich Verantwortlicher der Software sowie der im Rahmen des § 15a Abs. 6 zu führenden Dokumentationsverarbeitungen im Sinne der §§ 36 Abs. 2 Z 8, 46 ff DSG und hat als solcher für das Überwachungsprogramm ein Verzeichnis von Verarbeitungstätigkeiten zu führen (vgl. §§ 4, 49 DSG), mit der Datenschutzbehörde nach Maßgabe des § 51 DSG zusammenzuarbeiten und eine Datenschutz-Folgenabschätzung durchzuführen (§ 52 DSG).

Gemäß § 15a Abs. 7 sind sämtliche ermittelte Nachrichten bereits während der Durchführung der Maßnahme zu prüfen und nur diejenigen Nachrichten weiterzuverarbeiten, die für die Abwehr jenes verfassungsgefährdenden Angriffs, für den die Maßnahme bewilligt wurde, erforderlich sind oder die nach § 15a Abs. 8 weiterverarbeitet werden dürfen. Daten, die demnach nicht weiterverarbeitet werden dürfen, sind nach den im Sicherheitspolizeibereich einschlägigen Bestimmungen (§ 63 SPG) zu löschen.

Sofern aus ermittelten Nachrichten, die nach Maßgabe des § 15a Abs. 7 erster Fall mangels Erforderlichkeit für die konkrete Aufgabenerfüllung prinzipiell zu löschen wären, Anhaltspunkte für eine begangene Straftat oder deren geplante Begehung zu Tage treten, eröffnet sich eine besondere Herausforderung im Spannungsverhältnis zwischen Offizialprinzip einerseits und dem Interesse an einer umfassenden Geheimhaltung der verdeckten Nachrichtenüberwachung andererseits. Um dem staatlichen Strafverfolgungsanspruch sowie der Verhinderung gefährlicher oder verfassungsgefährdender Angriffe dennoch Rechnung tragen zu können, soll die die Maßnahme durchführende Organisationseinheit nach § 1 Abs. 3 bei Bekanntwerden eines begründeten Gefahrenverdachts für einen anderen verfassungsgefährdenden Angriff im Sinne des § 11 Abs. 1 Z 8 – sprich eines solchen, für den die Überwachung von Nachrichten nach diesem Gesetz grundsätzlich zulässig wäre – als jenen, für den sie bewilligt wurde, um die Ermächtigung des Rechtsschutzbeauftragten für die Aufgabe nach § 6 Abs. 2 ansuchen. Bis dahin sind die betreffenden Nachrichten gesondert von den für die konkrete Aufgabenerfüllung erforderlichen Nachrichten zu verwahren. Sollte die Ermächtigung durch den Rechtsschutzbeauftragten verwehrt werden, sind die Nachrichten in nicht rückführbarer Weise zu löschen. Sollten sich aus den ermittelten Nachrichten Anhaltspunkte für ein von einem bestimmten Menschen geplantes (§ 16 Abs. 3 SPG) oder begangenes Verbrechen (§ 17 StGB) gegen Leben, Gesundheit, Sittlichkeit, Freiheit oder Vermögen ergeben, so ist darüber im Falle eines geplanten Verbrechens die zuständige Sicherheitsbehörde, im Falle eines begangenen die Staatsanwaltschaft, der die Entscheidung über Weiterführung, Beendigung oder Einstellung des Verfahrens sowie allenfalls einen Aufschub kriminalpolizeilicher Ermittlungen nach § 6 Abs. 4 Z 2 obliegt, ehestmöglich zu verständigen. Durch den Verweis auf § 16 Abs. 3 SPG soll klargestellt werden, dass auch gefährliche Angriffe, die sich noch im Vorbereitungsstadium befinden, von der Verständigungspflicht nach § 15a Abs. 8 Z 2 umfasst sind.

Die Schadenersatzbestimmung in § 15a Abs. 10 orientiert sich weitestgehend an der korrespondierenden strafprozessualen Bestimmung des § 148 StPO.

Zu § 17 Abs. 3:

Der Bundesminister für Inneres hat dem Ständigen Unterausschuss über die Durchführung von Nachrichtenüberwachungen nach § 11 Abs. 1 Z 8 oder 9 sowie die damit im Zusammenhang stehende Information Betroffener nach § 16 jedenfalls halbjährlich zu berichten.

Zu § 18 Abs. 9:

Es handelt sich um die Inkrafttretensbestimmung.