**Bundesgesetz, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz, das
Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, das
Bundesverwaltungsgerichtsgesetz und das Richter- und
Staatsanwaltschaftsdienstgesetz geändert werden**

Univ.-Ass. Mag. Daniel Oesterreicher

Mit 8.4.2025 langte der ME für eine Novelle des SNG, SPG, TKG 2021, BVwGG und RStDG im Nationalrat ein.¹ Die Begutachtungsfrist endet mit 3.6.2025.

Nachfolgend soll ein Überblick über die wichtigsten geplanten Änderungen geboten werden.²

I. Aufschiebung sicherheitspolizeilicher Einschreitens und kriminalpolizeilicher Ermittlungen

Mit der Novelle soll für den Aufgabenbereich des Verfassungsschutzes eine Möglichkeit zum Aufschiebung des sicherheitspolizeilichen Einschreitens (§ 6 Abs 4 Z 1 SNG) oder kriminalpolizeilicher Ermittlungen (§ 6 Abs 4 Z 2 SNG) geschaffen werden, wenn im Einzelfall ein überwiegendes Interesse an der Erfüllung der Aufgaben des Nachrichtendienstes oder Staatsschutzes besteht.

Für die weiteren Voraussetzungen eines Aufschiebung des sicherheitspolizeilichen Einschreitens wird auf § 23 Abs 1 und 3 SPG verwiesen. Ein Aufschiebung kriminalpolizeilicher Ermittlungen inklusive der Berichterstattung an die StA setzt voraus, dass mit dem Aufschiebung ex ante betrachtet keine ernste Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit Dritter verbunden ist.³ Die Gründe für den Aufschiebung sind zu dokumentieren und im Fall der Z 2 binnen sechs Monaten der StA als Bericht zu übermitteln.

II. Flexibilisierung der strikten Trennung zwischen Nachrichtendienst und Verfassungsschutz

Das SNG normiert grundsätzlich eine strikte organisatorische Trennung zwischen den jeweils für den Nachrichtendienst und für den Staatsschutz zuständigen Organisationseinheiten. Zur Koordinierung der beiden Aufgabenbereiche ist innerhalb der Direktion eine Informationsschnittstelle eingerichtet.⁴ Wenn dies im Interesse einer raschen und zweckmäßigen Aufgabenerfüllung geboten ist, soll der Direktor aber in Zukunft den Aufgabenbereich Nachrichtendienst in zwei Fällen auch mit der Wahrnehmung des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen durch Einzelpersonen (§ 6 Abs 2 SNG) betrauen dürfen: Nach § 6 Abs 5 Z 1 SNG nF, wenn sich im Zuge einer erweiterten Gefahrenforschung der begründete Verdacht ergibt, dass

¹ [8/ME 28. GP](#).

² Siehe auch [ErlME 8/ME 28. GP](#).

³ ErlME 8/ME 28. GP 2.

⁴ ErlME 8/ME 28. GP 3.

von einem Mitglied der beobachteten Gruppierung die Gefahr eines verfassungsgefährdenden Angriffs ausgeht. Nach Z 2, wenn sich der Verdacht eines verfassungsgefährdenden Angriffs aus Informationen ergibt, die dem Aufgabenbereich Nachrichtendienst von inländischen oder ausländischen Behörden übermittelt wurden und die einer Verarbeitungsbeschränkung unterliegen, sodass die Informationen nach den Vorgaben der übermittelnden Stelle nur von mit nachrichtendienstlichen Aufgaben betrauten Organisationseinheiten verarbeitet werden dürfen.⁵

III. Ausweitung des Deliktatalogs verfassungsgefährdender Angriffe

Der Katalog verfassungsgefährdender Angriffe in § 6 Abs 3 SNG wird in seiner Z 3 um den Tatbestand des § 247b StGB („Religiös motivierte extremistische Verbindung“) und in seiner Z 4 um die Tatbestände des § 50 Abs 1a WaffG („illegaler Waffenhandel“), § 25 Abs 1 und 2 des Investitionskontrollgesetzes und § 103 StGB („Überlieferung an eine ausländische Macht“) ergänzt.

IV. Nachrichten- und Messenger-Überwachung

a. Neue Ermittlungsbefugnisse

In § 11 Abs 1 Z 8 SNG nF soll eine § 134 Z 3 StPO nachgebildete Ermittlungsbefugnis geschaffen werden, die es den Verfassungsschutzbehörden erlauben soll, neben Verkehrsdaten auch Kommunikationsinhalte zu überwachen. Z 9 erstreckt diese Befugnis auch auf die Überwachung verschlüsselter Kommunikation (insbesondere end-to-end verschlüsselte Messenger-Dienste). Zu diesem Zweck soll zukünftig auch die Infiltration des zu überwachenden Computersystems mittels einer Spionagesoftware erlaubt werden – ein Novum in der österreichischen Rechtsordnung.⁶

Die neuen Überwachungsbefugnisse sollen nach den Materialien neben herkömmlicher (Sprach- und SMS-)Telekommunikation auch sämtliche Nachrichten und Informationen, die über internetbasierte Apps übermittelt werden (zB WhatsApp, Telegram), über einen Cloud-Diensteanbieter an einen Cloud-Server übermittelte Datenpakete und die autonome Kommunikation zweier Endgeräte ohne menschliches Zutun (M2M-Kommunikation) inklusive der Datenübermittlung an Server im Rahmen von automatisierten Backups erfassen. Durch begleitende Änderungen des Telekommunikationsgesetzes 2021 sollen die für die allfällige Mitwirkung der Kommunikationsdiensteanbieter an der Nachrichtenüberwachung erforderlichen Anpassungen vorgenommen werden. Weiterhin nicht zulässig ist eine Online-Durchsuchung aller auf dem Computersystem lokal gespeicherter Daten. Dies soll durch die ausdrückliche Eingrenzung auf Nachrichten, die mit einem Übertragungsvorgang in Zusammenhang stehen, sowie durch die in § 15a Abs 3 SNG nF festgelegte Beschränkung der Überwachung auf künftige Zeiträume abgesichert werden.⁷

b. Materielle und formelle Voraussetzungen

⁵ ErlME 8/ME 28. GP 3.

⁶ ErlME 8/ME 28. GP 3 f.

⁷ ErlME 8/ME 28. GP 4.

Aufgrund des Spannungsverhältnisses zu Art 8 EMRK stehen die neuen Ermittlungsbefugnisse den Verfassungsschutzbehörden nur zur Vorbeugung besonders schwerwiegender verfassungsgefährdender Angriffe zur Verfügung. Konkret eröffnen nur solche verfassungsgefährdenden Angriffe den Anwendungsbereich der neuen Überwachungsmaßnahmen, die im Falle ihrer Verwirklichung zumindest mit zehn Jahren Freiheitsstrafe bedroht wären sowie der Tatbestand des § 256 StGB („Geheimer Nachrichtendienst zum Nachteil Österreichs“).⁸ Darüber hinaus muss es für die Verfassungsschutzbehörden aussichtslos sein, ihre Aufgaben durch andere, weniger eingriffsintensive Ermittlungsmaßnahmen zu erfüllen. Die gleichlautenden Formulierungen in den Z 2, 3, 5, und 7 entfallen bzw werden sie durch die Formulierung „ansonsten wesentlich erschwert“ ersetzt. Damit soll allerdings keine Herabsetzung der Zulässigkeitsvoraussetzungen dieser Bestimmungen verbunden sein, sondern klargestellt werden, dass zukünftig die neuen Ermittlungsbefugnisse nach Z 8 und 9 die Stellung als ultima-ratio Maßnahmen im Bereich des Verfassungsschutzes einnehmen werden.⁹

In formeller Hinsicht müssen die Ermittlungsmaßnahmen nach Z 8 und 9 gemäß § 15a Abs 1 SNG nF auf Antrag der DSN vorab vom Bundesverwaltungsgericht bewilligt werden.¹⁰ Noch vor der Beantragung der gerichtlichen Bewilligung ist gemäß § 14 Abs 5 der Rechtsschutzbeauftragten („RSB“) zu befassen und ist diesem Gelegenheit zur Äußerung zu geben. Nach § 15a Abs 2 darf die Bewilligung nur in jenem Umfang (bezogen auf konkrete Übertragungsarten und Applikationen) und nur für jenen künftigen Zeitraum erteilt werden, der zur Aufgabenerfüllung voraussichtlich erforderlich ist.¹¹ Die Bewilligung darf für höchstens drei Monate erteilt werden. Eine Verlängerung setzt einen erneuten Antrag der DSN nach § 15a Abs 1 voraus.

c. Durchführung und technische Sicherheitsvorkehrungen

§ 15b SNG enthält detaillierte Bestimmungen zur Durchführung der neuen Überwachungsmaßnahmen. Nach Abs 1 werden technische Schutzvorkehrungen zu treffen sein, um sicherzustellen, dass eine über den Bewilligungsumfang oder Bewilligungszeitraum hinausgehende Überwachung vor vornherein nicht möglich ist (Z 1), am infiltrierten Computersystem nur unerlässliche Veränderungen vorgenommen werden (Z 2) und die Spionage-Software nach Beendigung der Ermittlungsmaßnahme vollständig entfernt oder funktionsunfähig gemacht wird (Z 3). Zudem sind dem Stand der Technik entsprechende Maßnahmen zu ergreifen, um die Spionage-Software vor unbefugter Nutzung und die ermittelten Nachrichten gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. § 15b Abs 2 SNG sieht eine umfassende Dokumentationspflicht vor, um die Authentizität und Integrität der erhobenen Nachrichten sowie die Nachverfolgbarkeit der Datenermittlung zu gewährleisten.¹²

Nach § 15b Abs 3 SNG sind sämtliche ermittelten Nachrichten und Informationen bereits während der Durchführung der Ermittlungsmaßnahme dahingehend zu überprüfen, ob

⁸ ErlME 8/ME 28. GP 4.

⁹ ErlME 8/ME 28. GP 3.

¹⁰ Eingriffe in das Fernmeldegeheimnis gemäß Art 10a StGG stehen unter einem Richtervorbehalt.

¹¹ ErlME 8/ME 28. GP 9.

¹² ErlME 8/ME 28. GP 10.

diese weiterverarbeitet werden dürfen. Daten, die nicht weiterverarbeitet werden dürfen, sind zu löschen. Eine Weiterverarbeitung ist zulässig, wenn die Nachrichten und Informationen für die Vorbeugung jenes verfassungsgefährdenden Angriffs, für den die Maßnahme bewilligt wurde, erforderlich sind. Abs 4 enthält eine ergänzende Regelung für Zufallsfunde. Eine Weiterverarbeitung ist auch dann zulässig, wenn sich aus den ermittelten Nachrichten Hinweise auf einen begründeten Verdacht für einen anderen verfassungsgefährdenden Angriff oder eine im Rahmen der erweiterten Gefahrenforschung zu beobachtende Gruppierung im Sinne des § 6 Abs 1 SNG ergeben und der RSB die Weiterverarbeitung der Zufallsfunde genehmigt. Ergeben sich aus den ermittelten Nachrichten Hinweise auf ein geplantes oder begangenes Verbrechen, ist die zuständige Sicherheitsbehörde oder Staatsanwaltschaft zu verständigen.

Schließlich enthält Abs 5 eine an § 148 StPO orientierte Schadenersatzbestimmung.¹³ Der Bund haftet für vermögensrechtliche Nachteile, die durch die Durchführung der Nachrichtenüberwachung nach dem SNG entstanden sind, außer der Geschädigte hat die Durchführung der Ermittlungsmaßnahme vorsätzlich herbeigeführt. Es gilt das AHG.

d. Kontrolle und Rechtsschutz

Die Novelle etabliert ein neuartiges Rechtsschutzsystem, welches sich einerseits aus der gerichtlichen Bewilligung der Überwachungsmaßnahme durch das BVwG und andererseits aus weitreichenden Rechtsschutzkompetenzen des RSB zusammensetzt (§ 14 Abs 5 iVm § 15a SNG).¹⁴

Dem RSB obliegt zunächst die Prüfung der gerichtlichen Bewilligung des BVwG, wobei er gemäß § 15c Abs 1 berechtigt ist, gegen die Bewilligung Revision beim Verwaltungsgerichtshof zu erheben. Im Weiteren ist der RSB auch für die laufende Kontrolle der Überwachungsmaßnahme, insbesondere in Hinblick auf deren Verhältnismäßigkeit und die Einhaltung der Grenzen der Bewilligung, zuständig. Zu diesem Zweck gewährt ihm § 15c Abs 2 ein umfassendes Einsichtsrecht in alle ermittelten Nachrichten, das Recht, die Löschung von Nachrichten zu verlangen sowie das Recht, bei Bedenken gegen die Verhältnismäßigkeit der Maßnahme beim BVwG die Aufhebung der Bewilligung zu beantragen. § 15c Abs 3 bis 5 enthalten ergänzende Regelungen, um die Vertraulichkeit der Überwachungsmaßnahme auch im Bereich des Rechtsschutzes zu gewährleisten. Zu diesen zählen die Nutzung sicherer Kommunikationskanäle, die Entscheidung des BVwG ohne Durchführung einer mündlichen Verhandlung und verpflichtende Vertrauenswürdigkeitsprüfungen für Mitglieder des BVwG und deren Bedienstete, soweit diese mit der Wahrnehmung von Aufgaben nach dem SNG betraut sind.

Nach Ablauf des Bewilligungszeitraums ist der Betroffene gemäß § 16 Abs 2 SNG von der Durchführung der Nachrichtenüberwachung nach § 11 Abs 1 Z 8 oder 9 zu informieren. Andere Personen sind dann zu informieren, wenn an sie oder von ihnen gesendete, übermittelte oder empfangene Nachrichten weiterverarbeitet wurden und ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist. Ein Aufschub der

¹³ ErlME 8/ME 28. GP 10.

¹⁴ ErlME 8/ME 28. GP 10 f.

Benachrichtigung ist nach Abs 3 mit Zustimmung des RSB möglich, wenn und solange diese die Aufgabenerfüllung gefährden würde.

e. Sonstiges

In § 11 Abs 1 Z 7 SNG soll schließlich eine Rechtsgrundlage für den Einsatz von technischen Mitteln, insbesondere WLAN-Catchern, geschaffen werden, mit denen Verkehrs-, Zugangs- und Standortdaten auch ohne Einbeziehung von Betreibern bzw Diensteanbietern ermittelt werden können.¹⁵

v. Änderungen des SPG

In § 91b SPG soll einerseits eine verpflichtende Vertrauenswürdigkeitsprüfung des Rechtsschutzbeauftragten und seiner Stellvertreter (Abs 1a) sowie der sonstigen administrativen Mitarbeiter (Abs 3) vorgesehen werden.

Zudem soll in einem neuen Abs 2a eine Möglichkeit zur Abberufung des Rechtsschutzbeauftragten bzw seiner Stellvertreter durch den Bundespräsidenten im Falle grober Pflichtverletzungen oder einer nachträglichen Unvereinbarkeit mit der Funktion verankert werden.

VI. Änderungen des BVwGG und RStDG

Schließlich soll durch die Anpassungen im Bundesverwaltungsgerichtsgesetz (§ 16a BVwGG) und im Richter- und Staatsanwaltschaftsdienstgesetz (§ 66 Abs 3 RStDG) die Einführung einer Rufbereitschaft sowie eines Journaldienstes beim BVwG ermöglicht werden.

¹⁵ ErlME 8/ME 28. GP 4.