Bundesministerium für Inneres
Herrengasse 7
1010 Wien

per E-Mail: bmi-III-A-4-stellungnahmen@bmi.gv.at

Zl. 13/1 24/90

2024-0.148.142
BG, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird

Referent: MMag. Dr. Rupert Manhart, LL.M. (LSE), Rechtsanwalt in Bregenz

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag (ÖRAK) dankt für die Übersendung des Entwurfes und erstattet dazu folgende

Stellungnahme:

A. Vorbemerkungen

1. Hauptgegenstand des Entwurfs ist die Schaffung einer Rechtsgrundlage für die Überwachung verschlüsselter Nachrichten „zur effektiven Bekämpfung verfassungsschutzrelevanter Bedrohungslagen" (Erläuterungen 1). Die gegenständliche Stellungnahme befasst sich daher überwiegend mit dem Vorschlag für diese Regelung (§ 11 Abs 1 Z 9 SNG).

Die Überwachung von Nachrichten stellt einen Eingriff in grund- und menschenrechtlich geschützte Rechtspositionen betroffener Personen dar. So hielt der Verfassungsgerichtshof im Zuge der Aufhebung der Bestimmungen zum Bundestrojaner 2019 fest: *„Die verdeckte Überwachung der Nutzung von Computersystemen stellt einen schwerwiegenden Eingriff in die von Art. 8 EMRK geschützte Privatsphäre dar und ist nach Ansicht des Verfassungsgerichtshofes nur in äußerst engen Grenzen zum Schutz entsprechend gewichtiger Rechtsgüter zulässig*" (VfGH 11.12.2019, G 72-74/2019-48 und G 181-182/2019-18, Rz 180). Auch die nunmehr vorgeschlagene Regelung muss sich vor allem am Maßstab des Art 8 EMRK messen lassen. Demnach ist ein Eingriff in das Recht auf Achtung der Privatsphäre nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz

der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist (Art 8 Abs 2 EMRK).

Die österreichischen Rechtsanwältinnen und Rechtsanwälte verkennen nicht, dass der Schutz der Bevölkerung vor Terrorangriffen und die Bekämpfung des internationalen Terrorismus ein legitimes Ziel ist, das Eingriffe in die Privatsphäre rechtfertigen kann. Ein solcher Eingriff muss aber den **strengen Prüfungskriterien des Art 8 EMRK** genügen, also nicht nur auf einer gesetzlichen Grundlage beruhen und einen der in Art 8 Abs 2 EMRK aufgezählten legitimen Zwecken dienen, sondern auch in einer demokratischen Gesellschaft notwendig, also geeignet, erforderlich und angemessen sein, um den verfolgten legitimen Zweck zu erreichen.

Informationen, die den von Art 8 EMRK geschützten persönlichen Lebensbereich einer Person betreffen, sind von der Überwachung auszunehmen, soweit sie für die Erreichung des Zieles der Überwachungsmaßnahme nicht erforderlich sind. Sofern die Erlangung solcher, die Privatsphäre – etwa eines unbeteiligten Dritten – betreffender Informationen durch die Überwachungsmaßnahme unvermeidbar und im Lichte des Gewichtes und der Bedeutung des mit der Überwachungsmaßnahme verfolgten Zieles gerechtfertigt ist, hat der Gesetzgeber auf Ebene der Verwendung dieser Informationen Vorkehrungen zum Schutz des Rechtes auf Achtung des Privatlebens nach Art 8 EMRK zu treffen (VfGH 11.12.2019, G 72-74/2019-48 und G 181-182/2019-18, Rz 181).

Die Erläuterungen lassen weitestgehend im Dunklen, **welche konkreten Überlegungen** der Gesetzgeber in Bezug auf die Erforderlichkeit und Verhältnismäßigkeit angestellt hat. Es wird nur mit allgemeinen Worten darauf verwiesen, dass das Fehlen einer Möglichkeit zur effizienten Überwachung des Kommunikationsverkehrs die Aufgabenerfüllung der Verfassungsschutzbehörden erheblich erschwere.

2. Ein grundlegender Fehler der konkret ins Auge gefassten Regelung, die dem vorbeugenden Schutz vor verfassungsgefährdenden Angriffen – insbesondere im Hinblick auf die Abwehr geplanter terroristischer Anschläge – dienen soll, liegt darin, dass die **Schnittstelle zwischen den sicherheitspolizeilichen bzw nachrichtendienstlichen Erkenntnissen und dem Strafverfahren nicht ausreichend** geklärt ist. Eingriffe in Grundrechte, die der Vorbeugung von Angriffen dienen, sind an anderen Maßstäben zu messen als Eingriffe im Interesse der Strafverfolgung. Während die Prävention von schweren Straftaten weitergehende Eingriffe rechtfertigt, sind bei der Repression, also der Verwendung der Ergebnisse dieser Eingriffe im Interesse der Strafverfolgung wegen bereits erfolgter Straftaten, strengere Maßstäbe anzulegen, denn die geschützten Interessen sind in zweiterem Fall als weniger gewichtig anzusehen.

Die Erläuterungen (S 3) verweisen darauf, dass Erkenntnisse ausländischer Nachrichtendienste aufgrund ihrer Klassifizierung nur eingeschränkt für Strafverfolgungszwecke verwendet werden könnten. Gerade dies zeigt, dass rechtsvergleichende Überlegungen offenbar zu kurz greifen; es müssen nämlich immer Rechtsordnungen in ihrer Gesamtheit betrachtet werden. Wenn in anderen Ländern Nachrichtendiensten weitergehende Befugnisse eingeräumt werden, so ist dies grundrechtlich nur deshalb zulässig, weil eine klare Abgrenzung zwischen Prävention und Repression normiert ist und klare Regeln zur Verwendung derartiger Erkenntnisse in Strafverfahren existieren.

3. Es werden nicht zutreffende **technische Gegebenheiten** unterstellt und technische Aspekte verschwiegen, die zur Beurteilung wesentlich sind. Es bedarf einer technischen Analyse der Voraussetzungen zur Überwachung von Inhaltsdaten einer Kommunikation, ohne die die Folgen einer derartigen Maßnahme nicht beurteilt werden können.

Nachrichten können **während des Kommunikationsvorganges** entweder bei den Teilnehmerinnen und Teilnehmern der Kommunikation (Senderin bzw Sender oder Empfängerin bzw Empfänger) oder auf dem Transportweg (in der Kommunikationsinfrastruktur oder beim Provider) ausgespäht werden. Dies soll durch die in § 11 Abs 1 Z 8 und 9 vorgesehene „Überwachung von Nachrichten" erzielt werden. **Nach Abschluss des Kommunikationsvorgangs** können gespeicherte Nachrichten auf den Endgeräten der Teilnehmerinnen und Teilnehmer oder bei einem Provider, bei dem Daten gespeichert sind, ausgekundschaftet werden. Hierfür räumt das Strafprozessrecht entsprechende Befugnisse ein, die nicht Gegenstand dieser Stellungnahme sind.

Zunächst zur Überwachung von **prinzipiell offener Kommunikation,** die unverschlüsselt erfolgt: Auch wenn eine Transportverschlüsselung heutzutage zum Stand der Technik gehört, könnten derartige Nachrichten etwa beim Provider entschlüsselt, gelesen und überwacht werden. Klassische Telekommunikation (E-Mail, Telefon usw) fällt in diese Kategorie. Ein Dienst wie Telegram bedient sich (nur) einer Transportverschlüsselung, weshalb der Zugriff auf Telegram-Nachrichten bzw Gruppen technisch jedenfalls beim Provider selbst möglich wäre, der die Nachrichten entschlüsseln und lesen kann. Eine Kommunikation, die größere Gruppen erreichen möchte (wie Telegram), kann schon aus technischen Gründen nicht auf eine Peer-to-Peer-Verschlüsselung setzen, dies würde die Systeme und deren Ressourcen schlichtweg überfordern. § 11 Abs 1 Z 8 des Entwurfs zielt auf diese unverschlüsselte (also nicht „Peer-to-Peer" verschlüsselte) Kommunikation ab. Strafprozessual entspricht dies der „Überwachung von Nachrichten" (§ 134 Z 3 StPO), die unter engen Voraussetzungen (§ 135 Abs 3 StPO) nach richterlicher Bewilligung (§ 137 Abs 1 StPO), flankiert durch Rechte der bzw des Beschuldigten bzw Betroffenen (etwa auf Einsicht, § 139 StPO) und abgesichert durch ein Verwertungsverbot (§ 140 StPO) durchgeführt werden dürfen.

Die **verschlüsselte Kommunikation, die beim Versender verschlüsselt und erst bei der Empfängerin bzw beim Empfänger wieder entschlüsselt wird („Peer-to-Peer"),** ist während des gesamten Transportwegs sowie beim Provider für niemanden einsehbar. Sie wird etwa von WhatsApp und Signal eingesetzt. Die Verschlüsselung ist so stark, dass sie mit den Nachrichtendiensten zur Verfügung stehenden technischen Mitteln nicht – jedenfalls nicht in Echtzeit – entschlüsselt werden kann. Die einzige technische Möglichkeit, diese Nachrichten abzufangen, besteht daher durch Installation eines Computerprogramms auf dem Endgerät der Senderin bzw des Senders oder der Empfängerin bzw des Empfängers (eines Spähprogramms bzw „Trojaners"), wie dies in § 11 Abs 1 Z 9 des Entwurfs vorgesehen ist. **Eine strafprozessuale Entsprechung hierfür fehlt.** Technisch setzt dies voraus, dass eine Sicherheitslücke auf den jeweiligen Endgeräten besteht, die für die Installation, Steuerung und Kommunikation des Computerprogramms bzw mit diesem ausgenützt werden. Dieses Programm muss tief im System des Endgeräts implementiert werden und kann nicht nur einzelne Teile des Endgeräts überwachen.

4. Die technische Analyse zeigt die wesentliche Kritikpunkte am Entwurf:

Ausgenützt werden können **bestehende Sicherheitslücken**, die entweder auf Mängel im Endgerät bzw der Software zurückzuführen sind oder die absichtlich eingebaut werden.

Letzteres kann – wenigstens zugunsten eines „kleinen" Nachrichtendienstes wie des österreichischen, der keinen Einfluss auf die Hersteller hat – ausgeschlossen werden. Ungeplante Sicherheitslücken hingegen sollten nach Möglichkeit rasch aufgeklärt und geschlossen werden, denn sie sind nicht nur Zugangspunkt für das Spähprogramm (Trojaner), das von österreichischen Behörden eingesetzt wird, sondern auch für andere, fremde Dienste und nichtstaatliche Hacker.

Es ist wohl auszuschließen, dass nur österreichische Behörden eine Sicherheitslücke kennen, vielmehr wird diese auch für andere bekannt und ausnützbar sein. Durch **das Bestehen von Sicherheitslücken wird die österreichische Gesellschaft und Wirtschaft verletzlich**, sodass das Ansinnen der Behörden nicht auf das Ausnützen, sondern auf das Schließen gerichtet sein sollte, um die Resilienz der österreichischen Gesellschaft und Wirtschaft gegen digitale Angriffe zu erhöhen.

Technisch können Spähprogramme gar **nicht auf bestimmte Kommunikationsvorgänge beschränkt** werden. Sie können prinzipiell alle Vorgänge auf einem Endgerät erfassen. Auch werden solche Programme ja nicht von österreichischen Entwicklern selbst für die nationale österreichische Verwendung programmiert, sondern müssen aus dem Ausland zugekauft werden. Sie sind nicht auf die besonderen Anforderungen des österreichischen Rechts zugeschnitten, sondern eher auf die der jeweiligen Herstellernation (wie etwa USA, Israel usw), die andere Standards in Bezug auf Daten- und Persönlichkeitsschutz haben. Es ist daher eine reine Fiktion, dass auf technischer Ebene Spähprogramme so beschränkt und eingestellt werden (können), dass sie den gesetzlichen Anforderungen entsprechen. Schon aus technischen Gründen erfolgt ein umfassender Eingriff in die Privatsphäre der bzw des (unter Umständen unbeteiligten) Betroffenen.

5. Im Rahmen der grundrechtlich durchzuführenden Verhältnismäßigkeitsprüfung ist auf die **Erforderlichkeit einer derartigen Befugnis** zur Vorbeugung von Gefahren einzugehen. Die Erläuterungen schweigen auch hierzu, wohl mit gutem Grund: In der Vergangenheit war nachrichtendienstlich nämlich nicht das Fehlen von Informationen die Ursache dafür, dass Gefährdungen nicht erkannt wurden, sondern die ungenügende Verarbeitung und Analyse der ausreichend vorhanden Informationen.

Der Einsatz eines Spähprogramms kann sich außerdem nur gegen **bereits bekannte Gefährderinnen bzw Gefährder** richten. Eine **Massenüberwachung** ist gesetzlich nicht vorgesehen und würde auch die Ressourcen des Nachrichtendienstes übersteigen. Es müssen also bereits sehr gute Daten und Informationen vorliegen, bevor diese Ermittlungsmaßnahme überhaupt in Betracht gezogen werden kann. In diesem Fall funktionieren aber auch „klassische" Ermittlungsmaßnahmen, wie Observation und der Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 11 Abs 1 Z 1, 3 SNG) oder aber der Überwachung nicht verschlüsselter Kommunikation (wie von Telegram-Kanälen).

6. Auch das **Gewicht des Eingriffs** ist ein wesentliches Beurteilungskriterium: Die Möglichkeit, privat zu kommunizieren und Daten zu schützen, ist ein unabdingbarer Bestandteil eines demokratischen Rechtsstaats, der ihn von totalitären Überwachungsstaaten unterscheidet. Technisch erfolgt der Schutz der Privatsphäre durch Verschlüsselung, die private Daten und private Kommunikation vor dem Eingriff Dritter schützt. Dritte können dabei neben staatlichen Behörden auch fremde Mächte oder Kriminelle sein.

Elektronische Datenverarbeitung durchdringt jeden Aspekt unseres Lebens. Daten, die wir tagtäglich generieren, erlauben den **Einblick in all unsere Lebensbereiche**, auch in intimste Informationen und sensible Daten, die persönliche Vorlieben, Einstellungen und Gedanken betreffen.

Nicht übersehen werden darf, dass durch den Einsatz einer derartigen Software auch unbeteiligte Dritte berührt werden. Jede Kommunikation bzw Nachrichtenübermittlung betrifft zumindest zwei Personen.

Die Überwachung von Computersystemen ist daher ein schwerwiegender Eingriff in die Privatsphäre und kann nicht auf die leichte Schulter genommen werden.

7. Bemerkenswert ist, dass in dem vorliegenden Entwurf einige notwendige Regelungen und Bestimmungen völlig fehlen:

Es sind **keine Bestimmungen zum Schutz von Berufsgeheimnisträgerinnen bzw Berufsgeheimnisträgern** vorgesehen. Nachrichten, die die bzw der Betroffene etwa mit der eigenen **Rechtsanwältin** bzw dem eigenen **Rechtsanwalt** oder einer **Journalistin** bzw einem **Journalisten** austauscht, können ohne Einschränkung eingesehen und verwendet werden. Diese verletzt neben Art 8 EMRK auch weitere Grundrechte, so etwa die Grundsätze eines fairen Verfahrens (Art 6 EMRK).

Es fehlen Regelungen zur **Sicherung der Integrität der gewonnenen Informationen** und Überprüfung derselben im Strafverfahren. Ein Eingriff durch ein Spähprogramm bedingt nämlich eine Manipulation von Daten auf dem Endgerät, die dadurch gewonnenen Informationen können ohne Nachvollziehbarkeit verändert worden sein. Auch dies verletzt das Grundrecht auf ein faires Verfahren (Art 6 EMRK).

Schließlich fehlen **Bestimmungen in Bezug auf die Überprüfung der eingesetzten Programme.** Sie müssten unbedingt (extern) zertifiziert und geprüft werden, um sicherzustellen, dass sie den rechtlichen und technischen Voraussetzungen entsprechen.

B. Besonderer Teil

1. Zu § 11 Abs 1 (Ermittlungsmaßnahmen)

Die Regelung ist gewissermaßen das Herzstück des Entwurfs: In Z 8 und Z 9 werden die neuen Ermittlungsmaßnahmen eingeführt. Aber auch in den übrigen Ziffern werden wesentliche Änderungen vorgenommen, die in den Erläuterungen dazu nicht begründet werden. **Jede dieser Änderungen bezweckt, den Einsatz der Ermittlungsmaßnahmen zu erleichtern:**

- In Z 1 wird als Voraussetzung für den Einsatz technischer Mittel bei Observationen die Voraussetzung, dass die Observation „ansonsten aussichtslos" wäre, gestrichen.
- Bei verdeckten Ermittlungen (Z 2) wird ebenfalls die Subsidiarität zu anderen Ermittlungsmaßnahmen gestrichen.
- Der verdeckte Einsatz von Bild- und Tonaufzeichnungsgeräten (Z 3) soll zulässig sein, wenn die Aufgabenerfüllung ansonsten wesentlich erschwert wäre, statt wie bisher ansonsten aussichtlos.
- Auch bei Z 5 wird die Subsidiarität des Einsatzes technischer Mittel zur Ortung von Endgeräten (z.B. durch IMSI-Catcher) gestrichen.
- So genügt nun auch in Z 7, wenn der Einsatz der technischen Mittel „erforderlich erscheint".

Durch die Änderungen wird **in die Verhältnismäßigkeit der Maßnahmen** erheblich eingegriffen. Eine sachliche Begründung dafür ist nicht ersichtlich. Die Erläuterungen vermeinen nur, dass „Unklarheiten im Zusammenspiel von Ermittlungsmaßnahmen" hintangehalten werden müssten. Selbst wenn es praktische Anwendungsschwierigkeiten gäbe, müssten die Folgen der Änderung im Rahmen einer wirkungsorientierten Folgenanalyse evaluiert werden. Die Änderungen sind schon infolge der mangelnden Begründung der Änderungen und wegen deren Unverhältnismäßigkeit abzulehnen.

Z 8 normiert die **Überwachung unverschlüsselter Kommunikation** zur Vorbeugung verfassungsgefährdender Angriffe. Diese Überwachungsbefugnisse waren bislang den **Strafverfolgungsbehörden vorbehalten**, die unter engen Voraussetzungen (§ 135 Abs 3 StPO) nach richterlicher Bewilligung (§ 137 Abs 1 StPO), flankiert durch Rechte der bzw des Beschuldigten bzw Betroffenen (etwa auf Einsicht, § 139 StPO) und abgesichert durch ein Verwertungsverbot (§ 140 StPO) durchgeführt werden dürfen. Wenn auch nachvollziehbar erscheint, dass diese Befugnisse auch im Interesse der nachrichtendienstlichen Aufgabenerfüllung notwendig sind, so darf dies nicht dazu führen, dass auf **diesem Umweg Erkenntnisse in strafrechtliche Ermittlungen einfließen**, die nach der StPO nicht hätten gewonnen bzw verwertet werden dürfen (siehe dazu § 15a Abs 8 Z 2 des Entwurfs).

Dem vorgeschlagenen Z 9 stehen die zu Z 8 erhobenen Bedenken und in den Vorbemerkungen angeführten Überlegungen entgegen. **Das staatliche Hacken von Computersystemen ist aus den bereits dargelegten Überlegungen als unverhältnismäßiger Grundrechtseingriff abzulehnen.**

2. Zu § 14 Abs 5 SNG iVm § 15a Abs 9 SNG (begleitende Überwachung)

§ 14 Abs 5 SNG normiert (unter anderem) die begleitende Kontrolle der Durchführung der in § 11 Abs 1 Z 8 und 9 angeführten Ermittlungsmaßnahmen durch die Rechtsschutzbeauftragte bzw den Rechtsschutzbeauftragten. Die bzw der Rechtsschutzbeauftragte hat insbesondere darauf zu achten, dass während der Durchführung die Bewilligung nicht überschritten wird und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist.

Allerdings wurde verabsäumt, **der bzw dem Rechtsschutzbeauftragten für diese Aufgabe auch ausreichende Befugnisse und Ressourcen einzuräumen.** Zwar normiert § 15 Abs 1 SNG, dass ihr bzw ihm jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen sowie in die Datenverarbeitungen nach § 12 Abs 1 und 1a SNG zu gewähren und ihr bzw ihm auf Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen sind. Die bzw der Rechtschutzbeauftragte ist im Übrigen erst aber **nach Beendigung der Ermittlungsmaßnahme** nach § 11 Abs 1 Z 8 oder 9 ermächtigt, die weiterverarbeiteten Nachrichten einzusehen und anzuhören. Das Verhältnis dieser Regelungen kann nur so verstanden werden, dass die bzw der Rechtschutzbeauftragte zwar Rohdaten auch während der Ermittlungsmaßnahme einsehen kann, sie bzw er aber keinen Zugriff auf die daraus resultierenden Erkenntnisse in Form „weiterverarbeiteter Nachrichten" hat. Ohne Ressourcen personeller Natur, insbesondere auch mit der erforderlichen spezialisierten IT-Fachkenntnis, kann die Aufgabe nicht effektiv wahrgenommen werden.

Die laufende Überwachung ist unabdingbar, um wesentliche Rechte, vor allem in Bezug auf die Verhältnismäßigkeit des Eingriffs, den Schutz bestimmter Nachrichten, die von der

Überwachung nicht erfasst werden dürfen (die etwa Berufsgeheimnisse betreffen) und überhaupt die technischen Beschränkungen des eingebrachten Computerprogrammes und dessen korrekte Arbeitsweise betreffen. **Eine effektive begleitende Aufsicht** über die laufende Durchführung (VfGH 11.12.2019, G 72-74/2019-48, G 181-182/2019-19, Rz 192) ist damit **nicht gewährleistet**.

3. Zu § 14 Abs 4 und 5, 15 Abs 2, 15a sowie 16 Abs 2 (Rechtsschutz)

Die Erläuterungen führen aus, dass ein mehrstufiges Bewilligungs- und Kontrollverfahren unter Einbindung des Bundesverwaltungsgerichts vorgesehen sei. Es bestehen dennoch **Zweifel an der Effektivität dieses Rechtsschutzes:** Die bzw der Rechtsschutzbeauftragte kann zwar vor Genehmigung durch das BVwG eine Stellungnahme abgeben, es bleiben ihr bzw ihm dafür aber nur drei Tage Zeit und sie hat keinerlei Bindungswirkung. Die Bewilligung obliegt schließlich der Einzelrichterin bzw dem Einzelrichter, obgleich die Schwere des Eingriffs die Befassung zumindest eines Dreier-Senats indizieren würde.

Nach **Beendigung der Maßnahme** sind die bzw der Betroffene und Dritte zu informieren, also jene Personen, an die oder von denen Nachrichten gesendet, übermittelt oder empfangen wurden, die aufgrund ihrer Erforderlichkeit für die Aufgabenerfüllung weiterverarbeitet wurden. Diese sind aber nur zu informieren, sofern ihre Identität sich ohne besonderen Verfahrensaufwand, somit lediglich durch leicht durchführbare zusätzliche Erhebungen, feststellen lässt. Außerdem sind sie nur dann zu informieren, wenn ihre Nachrichten weiterverarbeitet wurden. Für einen Nachrichtendienst sollte es in der Regel kein besonderer Aufwand sein, die Identität der Teilnehmerinnen und Teilnehmer an einer elektronischen Kommunikation festzustellen, aber besondere Anstrengungen wird die DSN dafür nicht unternehmen. Außerdem geschieht der Eingriff bereits durch das Abfangen bzw Ausspähen, nicht erst durch das Weiterverarbeiten der Nachricht.

Zwar zählen die Erläuterungen die **Beschwerdemöglichkeiten** auf, diese werden aber der Situation nicht gerecht: Es wird nur auf datenschutzrechtliche Bestimmungen des SPG (§ 90 SPG) sowie Beschwerde nach § 88 Abs 2 SPG wegen Verletzung subjektiver Rechte verwiesen. Der bewilligende Beschluss selbst kann nur durch Revision an den VwGH bekämpft werden; zumal die Höchstgerichte keine Tatsacheninstanzen sind, ist eine solche Revision aber erheblich begrenzt.

4. Zu § 15a Abs 5 (technische Eigenschaften der Überwachungssoftware)

Bei der Durchführung einer Ermittlungsmaßnahme gemäß § 11 Abs 1 Z 9 ist technisch sicherzustellen, dass ausschließlich innerhalb des Bewilligungszeitraums gesendete, übermittelte oder empfangene Nachrichten überwacht werden können. Diese Vorschrift hat zwei wesentliche Aspekte, nämlich die **zeitliche Begrenzung** (auf den Bewilligungszeitraum) und die **inhaltliche Begrenzung (auf Nachrichten)**. Technisch können diese Voraussetzungen aber gar nicht sichergestellt werden, denn das Programm muss tief ins Zielsystem integriert werden, um seine Aufgaben erfüllen zu können. In einem Kommunikationsverlauf können auch ältere Nachrichten nicht einfach ignoriert werden.

5. Zu § 15a Abs 8 Z 2 (Weitergabe an Strafverfolgung)

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.

Es können daher **(zufällige) Ergebnisse der Nachrichtenüberwachung, die niederschwellige Bereiche** betreffen (die Einschränkung auf Verbrechen ist nicht ausreichend, zumal „Anhaltspunkte" hierfür leicht gesehen werden können), für sicherheitspolizeiliche Maßnahmen und strafrechtliche Ermittlungen herangezogen werden. Im Fall strafprozessualer Nachrichtenüberwachung wären die Anforderungen erheblich strikter. Die Regelung lädt zur **Umgehung** ein und verdeutlicht die **Missbrauchsanfälligkeit** der neuen Überwachungsbefugnisse. Sie verletzt auch den Grundsatz eines fairen Verfahrens, da die bzw der Betroffene **keine ausreichenden Rechtschutzmöglichkeiten** genießt. Eine Weitergabe von Informationen vor allem für Zwecke der Strafverfolgung hat zu unterbleiben.

C. Zusammenfassung und Fazit

1. Die geplante Regelung in Bezug auf die Überwachung von Nachrichten, und zwar sowohl der unverschlüsselten (§ 11 Abs 1 Z 8) als auch der unverschlüsselten Kommunikation stellen offensichtlich einen Eingriff in Art 8 EMRK, dem Grundrecht auf Schutz der Privatsphäre, dar, **der insbesondere den Anforderungen in Bezug auf die Verhältnismäßigkeit nach Art 8 Abs 2 EMRK nicht genügt.**

2. Die aus den technischen Aspekten resultierenden Kritikpunkte können auch durch Änderungen des Entwurfs nicht beseitigt werden. Kardinalfehler sind der Umstand, dass **IT-technische Sicherheitslücken** absichtlich offengehalten werden müssen, sowie die **Tiefe des Eingriffs in das Endgerät,** der nicht auf die bloße Überwachung von Kommunikation beschränkt werden kann. Der ÖRAK lehnt den Gesetzesentwurf daher ab.

3. Auch in rein rechtlicher Hinsicht besteht ein umfassender Änderungs- und Verbesserungsbedarf, nämlich insbesondere in Bezug auf folgende Regelungen:

- Fehlende Bestimmungen zum Schutz der Kommunikation mit **Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern** (Rechtsanwältinnen bzw Rechtsanwälten, Journalistinnen bzw Journalisten) sind nachzutragen.

- Die Bedingungen für die Verwendung von **Informationen in Strafverfahren** einschließlich von Regeln zur Sicherung der Integrität der Daten müssen klargestellt werden. Die gegenwärtigen Regelungen verletzen den Grundsatz eines **fairen Verfahrens**. Insbesondere ist vorzusehen, dass die Integrität der Daten überprüft und unzulässig verarbeitete Daten nicht verwendet werden dürfen.

- Um zu gewährleisten, dass Spähprogramme technisch strikt begrenzt sind, ist eine **externe Zertifizierung** von Spähprogrammen unabdingbar.

- Es müssen die **Rechtsschutzmöglichkeiten** verbessert werden, vor allem für durch die Überwachung betroffene Dritte.

- Die bzw der Rechtsschutzbeauftragte ist mit effektiven Möglichkeiten zur **begleitenden Überwachung** auszustatten; sie bzw er benötigt hierzu Ressourcen und vor allem IT-Fachkräfte.

Wien, am 24. September 2024

Der Österreichische Rechtsanwaltskammertag

Dr. Armenak Utudjian
Präsident