Universität für Weiterbildung Krems

Assoz.Prof. Dr. Walter Seböck, MSc MBA

Department für Sicherheitsforschung

T +43 (0)2732 893-2317
walter.seboeck@donau-uni.ac.at
www.donau-uni.ac.at/dsi

Bundesministerium für Inneres
Herrengasse 7
1010 Wien

bmi-III-A-4-stellungnahmen@bmi.gv.at

3. Juni 2025

Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz, das Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, das Bundesverwaltungsgerichtsgesetz und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden

Sehr geehrte Damen und Herren!

Das Department für Sicherheitsforschung an der Universität für Weiterbildung Krems erlaubt sich, mit Dank für die Anfrage, folgende punktuelle Anmerkungen zu übermitteln:

Ausgangslage und sicherheitspolitischer Kontext

Eine Analyse der vereitelten Anschlagsplanungen der letzten zwei Jahre in Österreich (Exemplarisch: Vienna Pride-Parade Anschlagsversuch Juni 2023, Szenario Hauptbahnhof September 2023, Silvesterpfad 2023, Taylor-Swift-Konzert-Anschlagsplanung August 2024 und zuletzt Westbahnhof Februar 2025) zeigt folgendes Ergebnis: In den genannten Fällen war es nur durch Hinweise internationaler Nachrichtendienste möglich, geplante Terroranschläge rechtzeitig zu verhindern. Die Erkenntnis ist, dass extremistische Gruppen diese verschlüsselten Messengerdienste nutzen, um anonym und abgeschirmt zu kommunizieren und die entscheidenden Informationen häufig durch das behördliche Mitverfolgen der Kommunikation von einschlägig dringend tatverdächtigen Extremisten auf verschlüsselten Messengerdiensten wie Telegram, Signal, Threema, WhatsApp oder Rocket.Chat gewonnen wurden.

Diese ausländischen Partnerdienste – insbesondere aus den USA, Großbritannien und Deutschland – übermittelten ihre Erkenntnisse an die österreichischen Staatsschutzbehörden. Ohne diese frühzeitigen Warnungen, die auf der gezielten und anlassbezogenen Überwachung digitaler Kommunikationskanäle beruhen, wären mutmaßlich mehrere geplante Anschläge zur Durchführung gekommen.

Universität für Weiterbildung Krems

Relevanz der Messengerdienst-Kommunikationsüberwachung im Bereich der Terrorismusbekämpfung

Insbesondere im extremistischen und terroristischen Spektrum hat sich die Kommunikation zunehmend in digitale Sphären verlagert – in verschlüsselte, schwer einsehbare virtuelle Räume. Täter und Mitwisser radikalisieren sich dort, tauschen taktische Planungsanleitungen, Propagandamaterial und logistische Informationen aus, die für die Umsetzung von Terroranschlägen benötigt werden. Die präventive Aufdeckung solcher Aktivitäten ist maßgeblich davon abhängig, dass Sicherheitsbehörden Zugang zu diesen Kommunikationsinhalten erhalten.

Internationale Vergleichsperspektive

Ein Vergleich mit anderen europäischen Ländern zeigt: Die meisten Staaten in der EU wie Frankreich, Großbritannien oder Deutschland verfügen über rechtliche Grundlagen zur Überwachung verschlüsselter Kommunikation im Bereich der Gefahrenabwehr und Terrorismusbekämpfung. Hierbei handelt es sich idR um richterlich autorisierte, zielgerichtete Maßnahmen, bei denen konkrete Gefahrenlagen oder relevante Verdachtsanhaltspunkte vorliegen müssen. Gerade das Beispiel Frankreich zeigt, dass durch den gezielten Einsatz technischer Lösungen zur Kommunikationsüberwachung zahlreiche Attentatsplanungen rechtzeitig erkannt und verhindert werden konnten – bei gleichzeitig gewahrt bleibendem rechtsstaatlichem Rahmen. Ebensolches gilt für Deutschland.

Technische Machbarkeit und rechtliche Absicherung

Ein wesentlicher Kritikpunkt in der aktuellen österreichischen Debatte um den gezielten Zugriff auf verschlüsselte Kommunikationsdienste bezieht sich auf die Erkenntnis des österreichischen Verfassungsgerichtshofs (VfGH) aus dem Jahr 2019. Damals wurde die gesetzliche Grundlage für die sogenannte "Bundestrojaner"-Regelung (§ 135a StPO) als verfassungswidrig aufgehoben – primär wegen mangelnder Verhältnismäßigkeit und unzureichender rechtlicher Eingrenzungen.

Allerdings beruht diese Kritik auf einem technischen und rechtlichen Verständnisstand, der zwischenzeitlich technisch und rechtlich überholt erscheint.

Technologischer Fortschritt seit 2019

Die damalige Gesetzeslage sah unter anderem die Möglichkeit vor, über Schadsoftware direkt in Endgeräte einzudringen – eine Maßnahme, die hohe Grundrechtseingriffe verursacht hätte. Seitdem hat sich die technische Diskussion jedoch deutlich weiterentwickelt. Heute stehen zielgerichtete, minimalinvasive Verfahren zur Verfügung, unter anderem etwa das sogenannte Client-Side Scanning (CSS), bei dem Inhalte direkt auf dem Endgerät überprüft werden, bevor sie verschlüsselt werden – unter Wahrung rechtsstaatlicher Schutzmechanismen. Diese Verfahren ermöglichen eine viel präzisere, kontrollierte und technisch begrenzte Auswertung – etwa nur bei konkretem Terrorverdacht und unter richterlicher Anordnung –, sodass die früher gerügten Mängel der Verhältnismäßigkeit und Eingriffstiefe aus unserer Sicht deutlich reduziert werden können.

Verbesserte rechtliche Konzepte

Auch rechtlich wurde seit 2019 intensiv an Reformmodellen gearbeitet, die eine verfassungs- und grundrechtskonforme Ausgestaltung der Kommunikationsüberwachung sicherstellen.

Universität für Weiterbildung Krems

§6 Abs4 SNG - E

In Bezug auf den vorliegenden Entwurf sehen wir die Überarbeitung der Regelung §6 Abs4 positiv. Die geplante Norm erfasst sowohl sicherheits- sowie kriminalpolizeiliche Aufgaben sowie die Aufgaben des Verfassungsschutzes. Diese Aufgaben waren davor nicht berücksichtigt. Aus unserer Sicht wäre es wünschenswert, die zugrundeliegenden Kriterien der Interessenabwägung des Aufschubs gem §23 darzustellen.

§6 Abs5 SNG - E

Die Neuregelung bzw der Vorschlag §6 Abs5 bietet die Möglichkeit, starre Aufgabenabläufe zu flexibilisieren und an die Erfordernisse der Praxis anzupassen. Aus unserer Sicht wäre es effektiver, in diesem Zusammenhang den Prozess der Information an den Rechtsschutzbeauftragen und der Einholung dessen Ermächtigung für die konkrete Aufgabe zu vereinheitlichen.

§11 Abs1 SNG – E

Z5 soll eine Anpassung an die korrespondierende Bestimmung der StPO (§ 134 Z 2a StPO) vornehmen, mittels derer 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 ohne Mitwirkung des Anbieters (oder sonstigen Diensteanbieters) handelt. Aus unserer Sicht ist dies zielführend.

§11 Abs1 Z8 und 9

Bekanntermaßen verfügen die Verfassungsschutzbehörden in Bezug auf die Telekommunikation gem SNG nur über die Möglichkeit, Verkehrsdaten zu ermitteln, nicht aber Kommunikationsinhalte. Da diese Möglichkeiten in anderen Ländern bestehen und die Inhaltsüberwachung nicht durch herkömmliche Ermittlungsmaßnahmen substituiert werden kann, sind die österreichischen Verfassungsschutzbehörden auf die Unterstützung durch ausländische Partnerdienste angewiesen. Da die Kommunikation im Allgemeinen zunehmend über verschlüsselte Plattformen abläuft und daher auch kriminelle und extremistische Nachrichten über diese Kanäle ausgetauscht werden, ist es 16 Jahre nach der Erfindung von WhatsApp, 13 Jahre nach Erfindung von Telegram und 11 Jahre nach Erfindung von Signal an der Zeit, den österreichischen Verfassungsschutz mit zeitgemäßen Ermittlungsmöglichkeiten auszustatten. Die Schaffung einer entsprechenden Rechtsgrundlage ist daher aus unserer Sicht ausgesprochen positiv. Aus unserer Sicht ist §11 Abs1 gut formuliert und deckt den Bedarf ab.

Gerade in diesem Zusammenhang verstehen wir die Kritikpunkte, die im Zusammenhang mit einer solchen Eingriffsmöglichkeit bestehen. Immerhin handelt es sich hierbei um einen massiven Grundrechtseingriff. Die Argumentation, wonach Überwachung zwar grundsätzlich nachvollziehbar sei, jedoch aus grundrechtlichen Gründen abzulehnen und daher auf traditionelle Ermittlungsformen zu verweisen sei – auch wenn diese die Aufklärung erheblich erschweren –, erscheint vor dem Hintergrund der Realität zynisch: Denn gleichzeitig wird die Nutzung von Informationen ausländischer Nachrichtendienste akzeptiert, die zur Erlangung dieser Informationen ihrerseits Grundrechte verletzt haben müssten. Diese Form indirekter Partizipation wirkt widersprüchlich und müsste konsequenterweise ebenfalls abgelehnt werden.

Universität für Weiterbildung Krems

Aus unserer Sicht sind relevante Kriterien in die neue Norm eingeflossen, bzw wurden berücksichtigt.

- Die inhaltliche Überwachung der Kommunikation soll nur im Einzelfall ermöglicht werden
- Die Überwachung wird auf schwerwiegende, verfassungsgefährdende Bedrohungen mit einem Strafrahmen von mindestens 10 Jahren Freiheitsstrafe bedroht ist, eingegrenzt
- Formales Kriterium ist eine richterliche Bewilligung über Beantragung der Maßnahme beim BVwG
- Vor Antragstellung ist der Rechtsschutzbeauftragte zu befassen
- Der Rechtsschutzbeauftragte hat drei Tage Zeit, eine Äußerung zu tätigen
- Der Rechtsschutzbeauftragte begleitet die Kontrolle

Technische Umsetzung
Eines der Probleme der Überwachung ergibt sich aus der technischen Umsetzung.

Verschiedene Expertisen gelangen zum Urteil, dass die technische Umsetzung nicht gesetzeskonform umsetzbar wäre. Weiters wird behauptet, dass ausländische Software zum Einsatz käme, die aus dubiosen Quellen stammt. Dies können wir nicht beurteilen, da noch kein Produkt in Diskussion steht.

Aus unserer Sicht wäre einer österreichischen Entwicklung der Vorzug zu geben, da dies zumindest in Bezug auf Datenmissbrauch durch Fremde bzw. ausländische Mächte oder Unternehmen, gewisse Grenzen zieht.

- Festlegung der Institution, die die Überwachung technisch sicherstellt,
- Sicherstellung, dass die verwendete Software keine Sicherheitslücken aufweist und Überwachungsdaten durch Dritte ausgelesen werden können,
- sowie eine technische Nichtweiterverwendbarkeit der Daten außerhalb des spezifischen Ermittlungszwecks und damit verbunden die detaillierte Beschreibung dieser zweckbindenden Technologie, der Prozesse, der Data Usage Control Frameworks und der involvierten Behörden.

Schlussfolgerung und Handlungsempfehlung
Die Auswertung von Messengerdienst-Kommunikation ist aus unserer Sicht kein Widerspruch zu liberalen Grundwerten, sondern ein notwendiges Instrument zur unmittelbaren Gefahrenabwehr im digitalen Zeitalter.

Universität für Weiterbildung Krems

In einem Umfeld, in dem extremistische Bedrohungen zunehmend digital, schnell und dezentral verlaufen, benötigen Sicherheitsbehörden Werkzeuge, die der Realität der Bedrohungslage gerecht werden. Ein Eingriff in die Grundrechte soll in funktionierenden Demokratien Diskussion wie eben diese auslösen und alle Bedenken in die Normerzeugung einfließen lassen.

Die Umsetzung ist idealerweise mit einer Evaluierungskomponente auszugestalten, die eine verpflichtende Überprüfung der Zweckmäßigkeit innerhalb einer bestimmten Frist vorsieht. Ergibt die Evaluierung Änderungsbedarf, sind entsprechende Anpassungen auf dieser Grundlage vorzunehmen.

Mit freundlichen Grüßen,

Walter Seböck