VEREINIGUNG DER ÖSTERREICHISCHEN RICHTERINNEN UND RICHTER

An das
Präsidium des Nationalrates
(https://www.parlament.gv.at/PERK/BET/VPBEST/#AbgabeStellungnahme)
An das Bundesministerium für Inneres
bmi-III-A-4-stellungnahmen@bmi.gv.at

Wien, am 25. September 2024

Betrifft: Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird (350/ME XXVII. GP)

GZ: 2024-0.148.142

Die Vereinigung der österreichischen Richterinnen und Richter erstattet unter Einbeziehung der Fachgruppen Grundrechte und interdisziplinärer Austausch, Strafrecht und Jugendstrafrecht folgende

Stellungnahme

zum oben genannten Gesetzesvorhaben.

Im Rahmen der Stellungnahme zum genannten Gesetzesentwurf auf zwei (neue) zentrale Befugnisse für den Aufgabenbereich des Staatsschutzes eingegangen. § 11 Abs 1 Z 8 SNG-ME soll die Überwachung von Telekommunikationsinhalten ermöglichen, während § 11 Abs 1 Z 9 SNG-ME den Zugriff auf verschlüsselt geführte Telekommunikation (wie etwa WhatsApp, Skype oder Signal) vorsieht. Bislang erlaubte das SNG den Verfassungsschutzbehörden lediglich die Ermittlung von Verkehrsdaten; Kommunikationsinhaltsdaten konnten hingegen nicht ermittelt werden.

Mit dem nunmehrigen Gesetzesentwurf wird für den Aufgabenbereich des Verfassungsschutzes die Möglichkeit geschaffen, in schwerwiegenden Einzelfällen nach

Schmerlingplatz 11, Postfach 26, A-1011 Wien
T +43 1 52152 303644, F +43 1 52152 303643
ute.beneke@richtervereinigung.at
www.richtervereinigung.at

richterlicher Bewilligung und unter begleitender wie nachprüfender Kontrolle anlassbezogen zur effektiven Bekämpfung von verfassungsschutzrelevanten Bedrohungslagen auch auf Kommunikationsinhalte zuzugreifen. Dieses Anliegen wird grundsätzlich begrüßt.

Die Schaffung neuer Ermittlungsmaßnahmen, die – wie vorliegend – intensive Eingriffe in Grundrechte ermöglichen, bedarf jedoch einer eingehenden grundrechtsspezifischen Abwägung. Solcherart müssen Überwachungsmöglichkeiten nicht nur rechtsstaatlichen Erfordernissen und grundrechtlichen Anforderungen entsprechen, sondern gleichzeitig auch ein überwiegendes Ziel, nämlich die Aufklärung schwerer Straftaten oder die Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit, verfolgen (vgl Art 8 Abs 2 EMRK). Die zu erfüllenden verfassungsrechtlichen Vorgaben im Hinblick auf die im ME vorgeschlagenen Regelungen in § 11 Abs 1 Z 8 und 9 SNG lassen sich insbesondere aus zwei Entscheidungen des Verfassungsgerichtshofs ableiten, zum einen VfGH 11.12.2019, G 72-74/2019 [„Aufhebung des § 135a StPO als verfassungswidrig"] und zum anderen VfGH 14.12.2023, G 352/2021 [„Handy-Sicherstellung"]. Dem erstzitierten Erkenntnis ist zu entnehmen, dass der VfGH die Ermittlungsmaßnahme der Überwachung (un-)verschlüsselter Nachrichten in seiner damaligen Entscheidung nicht grundsätzlich als grundrechtswidrig qualifizierte, vielmehr forderte er, dass eine derartige verdeckte Überwachung nur in Bezug auf Straftaten erfolgen dürfe, die im Einzelfall eine gravierende Bedrohung der in Art 8 Abs 2 EMRK genannten Ziele darstellen und einen solchen schwerwiegenden Eingriff rechtfertigen (vgl Rn 190 des genannten Erkenntnisses). Eine solcherart differenzierende Betrachtungsweise liegt auch der Entscheidung des VfGH in Bezug auf die Aufhebung der Sicherstellung zu Beweiszwecken gemäß § 110 Abs 1 Z 1 und Abs 4 StPO (iZm der „Handy-Sicherstellung") zugrunde.

Zu den materiellen und formellen Voraussetzungen der Inhaltsüberwachung nach § 11 Abs 1 Z 8 und Z 9 SNG-ME:

Der vorliegende Entwurf verlangt einen verfassungsgefährdenden Angriff (vgl zur hinreichenden Determinierung dieses Begriffs § 6 Abs 3 SNG), dessen Verwirklichung zumindest mit bis zu zehn Jahren Freiheitsstrafe bedroht ist und für den es einen begründeten Gefahrenverdacht (§ 6 Abs 2 SNG) geben muss. Dadurch ist sichergestellt,

dass die Überwachung sowohl von unverschlüsselten als auch verschlüsselten Nachrichten auf die Vorbeugung von gesetzlich umschriebenen, besonders schwerwiegenden verfassungsgefährdenden Angriffen beschränkt ist. Mit Blick auf die Voraussetzungen der Überwachung von Telekommunikationsinhalten nach § 135 Abs 3 StPO (vgl etwa Z 3 leg cit: „wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr bedroht ist“) wird die Eingriffsschwelle im SNG deutlich höher angelegt als in der StPO. Nach dem ME soll die Überwachung von Nachrichten zudem auch zur Vorbeugung eines „Spionagedelikts nach § 256 StGB“ zulässig sein. Vor dem Hintergrund der klaren, auf die Gefahr der Verwirklichung schwerwiegender Delikte im Zuständigkeitsbereich des Staatsschutzes abstellenden gesetzlichen Vorgaben ist eine uferlose Anwendung der in Rede stehenden Überwachungsmaßnahme auf Gesetzesebene ausgeschlossen.

Die Überwachung von (un-)verschlüsselten Nachrichten soll überdies nur dann zulässig sein, wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. Durch dieses zusätzliche Korrektiv wird der spezifischen Eingriffsintensität dieser Überwachungsmaßnahme ebenso Rechnung getragen. Zudem wird auch ein Rechtsschutzsystem im Sinne eines mehrstufigen Bewilligungs- und Kontrollverfahrens unter Einbindung des Bundesverwaltungsgerichts (vgl § 15a SNG-ME) und des beim Bundesminister für Inneres eingerichteten Rechtsschutzbeauftragten (vgl §§ 14 Abs 4 und 5 und 15 Abs 4 SNG-ME) etabliert.

Während bei der Überwachung unverschlüsselt kommunizierter Nachrichten nach § 11 Abs 1 Z 8 SNG-ME auf die im Rahmen des Vollzugs der Ermittlungsmaßnahme nach § 134 Z 3 StPO geschaffenen technischen Strukturen zugegriffen werden kann (hier ist kein zusätzlicher Eingriff in das Kommunikationsmedium der zu überwachenden Person erforderlich), ist für die Überwachung verschlüsselter Datenströme nach § 11 Abs 1 Z 9 SNG-ME zusätzlich die Einbringung eines Programms in das betreffende Computersystem notwendig. Ausgehend von§ 15a Abs 5 SNG-ME ist – in Anlehnung an § 100a Abs 5 der deutschen StPO – bei der Überwachung verschlüsselter Kommunikation sicherzustellen, dass ausschließlich innerhalb des Bewilligungszeitraums gesendete, übermittelte oder empfangene Nachrichten überwacht werden können (Z 1 leg cit). Solcherart sind die Behörden verpflichtet, darzulegen, dass durch die einzubringende Software lediglich auf

verschlüsselte Nachrichteninhalte innerhalb des mit der Bewilligung korrespondierenden Zeitraums zugegriffen und demzufolge nach dem Willen des Gesetzgebers gerade kein „Vollzugriff“ auf sämtliche Dateninhalte auf dem Quellgerät ermöglicht wird. Zudem sieht der Gesetzesentwurf vor, dass im Computersystem nur solche Veränderungen vorgenommen werden, die für die Nachrichtenüberwachung unerlässlich sind (Z 2 leg cit) und das Programm nach Beendigung entweder entfernt oder funktionsuntüchtig gemacht wird (Z 3 leg cit).

Während auf gesetzlicher Ebene die Voraussetzungen für die Überwachung (un-)verschlüsselter Nachrichten iSd § 11 Abs 1 Z 8 und 9 SNG-ME klar abgesteckt sind, bleibt die Frage der konkreten technischen Umsetzung bzw Machbarkeit einer Maßnahme nach § 11 Abs 1 Z 9 SNG-ME offen. So geht – wie Univ.-Prof. Dr. Robert Kert und Univ.-Ass. Dr. Raphaela Bauer-Raschhofer in ihrer Stellungnahme vom 28. August 2024 zum vorliegenden Gesetzesentwurf aufzeigen – beispielsweise der Verein epicenter.works davon aus, dass das gesamte Gerät „gehackt“ werden muss, um Zugriff auf verschlüsselte Nachrichten zu erhalten.

Demnach könnten sämtliche auf dem Gerät befindlichen Daten „wie Fotos, Dokumente, Standorte und auch niemals abgeschickte Nachrichtenentwürfe“ ausgelesen werden. Der Einsatz dieser Überwachungsmaßnahme werde zudem nur dann möglich sein, wenn „bestimmte Schwachstellen in Computersystemen bewusst nicht behoben werden und für das Einschleusen der Schadsoftware ausgenutzt werden“. Zuletzt wurde auch in einem im Der Standard erschienenen Gastkommentar vom 20. August 2024 („Die Verpippisierung des IT-Sicherheitsrechts“, Univ.-Prof. Dr. Nikolaus Forgó) kritisiert, dass der neue Gesetzesvorschlag zur Messengerüberwachung im SNG vieles zur technischen Umsetzung offen lasse und an den Grundfesten der (IT-)Sicherheit aller rüttle. Denn das Überwachen von Ende-zu-Ende verschlüsselter Kommunikation erfordere das Mithören an der Quelle, etwa am Handy, was wiederum deren Kompromittierung durch „nicht einfach so am Markt“ verfügbare „Schadsoftware“ verlange. Vor dem Hintergrund dieser (kritischen) Ausführungen zur technischen Effektuierung der in Rede stehenden Überwachungsmaßnahme ist besonders auf die Erwägungen des Verfassungsgerichtshofs in seinem § 135a StPO idF des Strafprozessrechtsänderungsgesetzes 2018 aufhebenden

Erkenntnis vom 11. Dezember 2019, G 72-74/2019, zu verweisen, der in seiner damaligen Entscheidung bei der Frage der Grundrechtskonformität der in Prüfung gezogenen Überwachungsmaßnahme (nach § 135a StPO) von den tatsächlichen Möglichkeiten der in ein Computersystem einzubringenden Software zur Überwachung verschlüsselter Nachrichten ausging und damit gerade nicht alleine auf die Intention des Gesetzgebers abstellte, bloß auf bestimmte Kommunikationsinhalte zuzugreifen. Solcherart machte der VfGH die Grundrechtskonformität der damals in § 135a StPO umschriebenen Überwachungsmaßnahme (auch) von den faktischen Möglichkeiten der einzubringenden Software abhängig (vgl Rn 183 des erwähnten Erkenntnisses; *Oswald*, ÖZW 2020, 87). Zur abschließenden Beurteilung der Verfassungskonformität der in § 11 Abs 1 Z 9 SNG geplanten Überwachung verschlüsselter Nachrichten wäre sohin zunächst klarzustellen, welche faktischen Zugriffsmöglichkeiten die einzubringende Software erlaubt, bzw wie die in Rede stehende Maßnahme technisch umgesetzt werden soll.

Die bereits oben angesprochenen Schranken für die eingesetzte Technologie sind zwar in § 15a Abs 5 SNG-ME normiert, zudem ist ausdrücklich vorgeschrieben, dass „das eingebrachte Programm (…) nach dem Stand der Technik gegen unbefugte Nutzung zu schützen“ ist. Allerdings gibt es in den weiteren Vorschriften zum „Besonderer Rechtsschutz bei der Überwachung von Nachrichten“ keinerlei Sicherungsvorkehrungen, wie die Einhaltung der Schutzbestimmungen des Abs 5 leg cit in der Praxis überprüft und sichergestellt wird. Hierzu wäre erforderlich, spezielle Aufsichtsbestimmungen für eine unabhängige Kontrolle der technologischen Umsetzung zu ergänzen.

Einen Vergleich bieten hierzu beispielsweise die Aufsichtsregelungen zum nationalen Teil des Schengen-Informationssystems (N.SIS). Die VERORDNUNG (EU) 2018/1862 des europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission, schreibt in Artikel 69 vor: „Die

Aufsichtsbehörden gewährleisten, dass die Datenverarbeitungsvorgänge in ihrem N.SIS mindestens alle vier Jahre nach internationalen Prüfungsstandards überprüft werden. Die Prüfung wird entweder von den Aufsichtsbehörden durchgeführt, oder die Aufsichtsbehörden geben die Prüfung unmittelbar bei einem unabhängigen Datenschutzprüfer in Auftrag. Der unabhängige Prüfer arbeitet jederzeit unter der Kontrolle und der Verantwortung der Aufsichtsbehörden."

In Österreich kommt diese Aufgabe der Datenschutzbehörde zu. Hier soll keine Präferenz für die Aufsichtszuständigkeit einer bestimmten Behörde zum Ausdruck kommen. Wichtig ist aber jedenfalls sicherzustellen, dass es eine unabhängige und fachlich qualifizierte Stelle gibt, die wohl auch die Vorgaben der Vertrauenswürdigkeitsprüfung nach dem SNG erfüllen müsste. Hier würden verschiedene bereits existierende und staatsnahe Einrichtungen in Frage kommen, wie beispielsweise CERT.at oder das Austrian Institute of Technology (AIT). Letztlich könnte aber nur durch ein unabhängiges Audit auf der konkreten technischen Umsetzungsebene durch entsprechende Sachverständige überprüft werden, inwieweit die rechtlichen Vorgaben auch tatsächlich umgesetzt sind.

Diese Art des kommissarischen (systemischen) Rechtsschutzes ist vor allem deshalb wichtig, weil die Software zur Umsetzung der geplanten Ermittlungsinstrumente auf dem Markt von privaten Anbietern zugekauft und nicht unter staatlicher Kontrolle entwickelt wird. Ein erstes Audit sollte daher im „Besonderen Rechtsschutz" schon vor dem realen Einsatz der Technologie im Zuge der Anschaffung und Implementierung verpflichtend vorgeschrieben und Teil eines Genehmigungsprozesses sein. Anders lässt sich die Gesetzmäßigkeit der technischen Umsetzung in der Praxis kaum sicherstellen. Eine Zielsetzung einer solchen Auditierung könnte neben dem Rechtsschutz für künftige Betroffene auch der Aspekt der Souveränität der Republik Österreich sein. Immerhin sollen hier in einem hochsensiblen Bereich des Verfassungsschutzes neuartige Technologien zum Einsatz gelangen, denen auch die Direktion für Staatsschutz und Nachrichtendienst (DSN) schon im eigenen Interesse nicht blind vertrauen sollte. In diesem

Zusammenhang sei an den nicht sehr weit zurückliegenden Skandal rund um die Spionage-Software „Pegasus“ erinnert.[1]

Die Reaktion des Europäischen Parlaments in Form einer kritischen Resolution ist nach wie vor einschlägig sowie aktuell und harrt ihrer Erfüllung durch die Mitgliedsstaaten.[2] Österreich hätte hier die Chance, eine Vorbildwirkung innerhalb der EU zu entfalten.

Zusammengefasst kann derzeit technisch nicht sichergestellt werden (und es ist daher „rechtliche Fiktion“), dass nur Teile der Kommunikation eines Mobiltelefons (z.B. beschränkt auf 2024) ausgelesen werden können, denn Zugriffe mittels Trojaner erfolgen stets auf das gesamte Gerät.

Überdies besteht eine Massengefährdung der IT-Sicherheit, wenn

- Sicherheitslücken künftig nicht mehr geschlossen werden, um Trojaner zu implementieren;

- private Experten im IT-Bereich diese Lücken künftig gar nicht mehr melden werden/wollen.

Zudem bestehen technische Möglichkeiten, sich einer Überwachung durch Einbringen eines derartigen Programms von vornherein zu entziehen und müsste der Trojaner kostspielig immer wieder neu implementiert werden, wenn das Mobiltelefon neu gestartet wird.

Die geschilderten technischen Parameter beeinflussen die Beurteilung der grundrechtlichen Verhältnismäßigkeit und nähren die Befürchtung, dass das Gesetz Überwachungsmöglichkeiten verspricht, die in der Praxis nur eingeschränkt und mit der Gefahr negativer Auswirkungen für die IT-Sicherheit im Gesamten erzielbar sind.

Dr. Gernot Kanduth

Präsident

---

[1] https://www.tagesschau.de/ausland/europa/pegasus-bericht-eu-100.html (17.09.2024)

[2] https://www.europarl.europa.eu/news/de/press-room/20231117IPR12230/spyware-meps-slaminsufficient-eu-response-to-abuse (17.09.2024)