An das
Bundesministerium für Inneres
Abteilung III//A/4
Herrengasse 7
1010 Wien

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

Wien, am 28.05.2025

Stellungnahme der ISPA zum Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, im Zusammenhang mit der öffentlichen Konsultation (Geschäftszahl: 2025-0.272.220) des Bundesministeriums für Inneres zum Entwurf eines Bundesgesetzes mit dem das Staatsschutz- und Nachrichtendienstgesetz (SNG), das Telekommunikationsgesetz 2021 (TKG 2021), das Sicherheitspolizeigesetz (SPG) und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden soll, wie folgt Stellung zu nehmen:

Der vorliegende Entwurf geht auf eine lange öffentliche Debatte zurück, in deren Rahmen von den staatlichen Sicherheitsbehörden wiederholt auf unzulängliche nachrichtendienstliche Befugnisse hingewiesen und insbesondere der Wunsch nach der Überwachung verschlüsselter Kommunikation geäußert wurde. Zentraler Bestandteil des Entwurfs ist die Ermächtigung der Direktion für Staatsschutz und Nachrichtendienst (DSN), eine staatliche Überwachungssoftware auf den Geräten sogenannter Gefährder zu installieren. Der Einsatz dieser Software wird laut Entwurf auf besonders schwerwiegende Bedrohungen – etwa Terrorismus oder Spionage – beschränkt und bedarf einer richterlichen Genehmigung sowie der Kontrolle durch einen Rechtsschutzbeauftragten. Die ISPA sowie die Netzbetreiber unterstützen die Sicherheitsbehörden bei der Wahrnehmung ihrer Aufgaben, insbesondere zum Schutz der Bürger:innen. Dabei ist die ISPA selbstverständlich bereit, eine konstruktive Zusammenarbeit anzustreben, jedoch stets unter der klaren Prämisse, dass die Grundrechte gewahrt und der Grundsatz der Verhältnismäßigkeit uneingeschränkt beachtet wird.

Die dem Entwurf vorausgehende Diskussion zur „Messenger-Überwachung“ spiegelt zwei schwer miteinander zu vereinbarende Interessen wider. Auf der einen Seite steht das Anliegen der staatlichen Sicherheitsbehörden, die zum Schutz der Bürger:innen und zur Abwehr verfassungsgefährdender Angriffe verpflichtet sind. Angesichts des technologischen Wandels in der Kommunikation möchten sie ihre gesetzlichen Befugnisse an die neuen Gegebenheiten anpassen, um mit den technischen Möglichkeiten der überwachten Personen Schritt halten zu können. Auf der anderen Seite steht das gesamtgesellschaftliche Interesse an privater und

verschlüsselter Kommunikation sowie an sicheren Informationsinfrastrukturen, verbunden mit der Sorge vor einem möglichen Missbrauch dieser Befugnisse. Zusätzlich zur rechtspolitischen Diskussion müssen auch klare verfassungsrechtliche Schranken beachtet werden, wie sie der österreichische Verfassungsgerichtshof in seinem Erkenntnis vom 11. Dezember 2019 formuliert hat, mit dem er das 2018 beschlossene „Sicherheitspaket", das ebenfalls Befugnisse zur Überwachung verschlüsselter Kommunikation enthielt, aufgehoben hat.[1]

Sofern der Einsatz einer Überwachungssoftware zur Anwendung kommt, hält die ISPA jede gesetzlich verankerte Einschränkung des Einsatzbereichs sowie eine mehrstufige Kontrolle für zwingend erforderlich. Gleichzeitig bestehen weiterhin erhebliche grundrechtliche Bedenken – insbesondere im Hinblick auf das Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK sowie das Recht auf Datenschutz gemäß § 1 DSG. Besondere Besorgnis besteht zudem hinsichtlich der Gefahr, dass durch den erweiterten Einsatz von IMSI- und WLAN-Catchern faktisch eine Vorratsdatenspeicherung eingeführt werden könnte. Daneben werfen auch sicherheitstechnische Aspekte erhebliche Fragen auf, insbesondere aufgrund der unklaren technischen Ausgestaltung sowie der fehlenden unabhängigen Kontrolle der eingesetzten Überwachungssoftware. Im Zusammenhang mit dem Einsatz einer staatlichen Überwachungssoftware ergibt sich somit ein grundlegendes Spannungsverhältnis zwischen dem berechtigten Ziel der Gefahrenabwehr und den damit einhergehenden Risiken, insbesondere der Gefährdung der gesamten digitalen Infrastruktur.

Die ISPA kann in ihrer Stellungnahme nicht auf sämtliche Aspekte dieser Debatte eingehen. Als Vertreterin der österreichischen Internetwirtschaft beschränkt sie sich dabei grundsätzlich auf die Wiedergabe der Perspektive der betroffenen Unternehmen und auf offene Fragen, die sich aus dem Entwurfstext ergeben. Im ersten Teil der Stellungnahme werden die sicherheitstechnischen Bedenken eingehend erörtert, während im zweiten Teil die grundrechtlichen Fragestellungen näher betrachtet werden. Die ISPA hofft, dadurch ihren Beitrag im Diskurs zu leisten.

I. Sicherheitstechnische Bedenken

Technische Durchsetzbarkeit der rechtlichen Vorgaben

Der Entwurf sieht in § 15b Abs 1 SNG vor, dass die Funktion der eingesetzten Überwachungssoftware technisch beschränkt sein muss. Die verwendete Überwachungssoftware darf ausschließlich Nachrichten überwachen, die innerhalb des bewilligten Zeitraums und im Rahmen des genehmigten Umfangs gesendet oder empfangen werden. Nach Abschluss der Maßnahme ist sie zu deaktivieren. In der Praxis ist es nach übereinstimmender Auffassung zahlreicher IT-Sicherheitsexperten jedoch nahezu unmöglich, die tatsächliche Funktionsweise einer solchen Überwachungssoftware vollständig zu

[1] VfGH 11.12.2018, G73/2019 ua.

kontrollieren oder verlässlich sicherzustellen, dass diese ausschließlich im gesetzlich zulässigen Rahmen operiert.[2] Denn die bislang bekannten und in der Praxis eingesetzten Überwachungsprogramme sind grundsätzlich in der Lage auf sämtliche Inhalte des betroffenen Endgeräts zuzugreifen – unabhängig davon, in welchem Umfang die Überwachungsmaßnahme genehmigt wurde.[3] Bereits daraus ergibt sich ein systemimmanentes Spannungsverhältnis zwischen rechtlicher Normierung und technischer Realität.

Ein weiteres, ebenso schwerwiegendes Problem ist das erhebliche Missbrauchspotenzial solcher Technologien. Mit der zunehmenden technischen Leistungsfähigkeit wächst das Risiko, dass solche Instrumente über den ursprünglich vorgesehenen Rahmen hinaus eingesetzt werden.

Ein Blick über die Grenze nach Ungarn verdeutlicht, welche Gefahren damit für Demokratie und Rechtsstaat einhergehen können: Dort wurde bekannt, dass die umstrittene Spionagesoftware *Pegasus* auf dem Mobiltelefon von Investigativjournalisten entdeckt wurde.[4] Auch in Polen wurde im April 2024 öffentlich, dass die frühere polnische Regierung offensichtlich die damalige Opposition während des Wahlkampfes unrechtmäßig überwachen ließ.[5] Derartige Vorgänge führen nicht nur zu erheblicher internationaler Kritik aufgrund des gravierenden Eingriffes in die Grundrechte betroffener Person – etwa die Pressefreiheit –, sondern illustrieren das erhebliche Missbrauchspotenzial staatlicher Überwachungstechnologien.

Diese Fälle in EU-Mitgliedsstaaten werfen die grundlegende Frage auf, wie sich der Einsatz einer hochsensiblen Überwachungssoftware mit den Prinzipien eines demokratischen Rechtsstaats vereinbaren lässt – vor allem dann, wenn es an Transparenz, wirksamer Kontrolle und klaren rechtlichen Schranken mangelt oder diese zu schwach ausgeprägt sind. Das Grundrecht auf Datenschutz, der Schutz der Privatsphäre sowie zentrale rechtsstaatliche Prinzipien bleiben damit unzureichend abgesichert.

Fehlende Kontrolle über die eingesetzte Überwachungssoftware

Ein zentrales Problem erkennt die ISPA in der Frage nach der Herkunft und der damit einhergehenden Kontrolle der eingesetzten Überwachungssoftware sowie die Sicherstellung der im Entwurf vorgesehenen rechtlichen Beschränkungen. Da derzeit davon auszugehen ist, dass die Direktion für Staatsschutz und Nachrichtendienst (DSN) die Überwachungssoftware

---

[2] CERT.at, 03.09.2024: *Ein paar Gedanken zur „Überwachung verschlüsselter Nachrichten*. Online abrufbar unter CERT.at Ein paar Gedanken zur „Überwachung verschlüsselter Nachrichten“.

[3] Der Kurier, 22.04.2025: *Mit List und Lücken zur Messenger-Überwachung.* Online abrufbar unter Mit List und Lücken zur Messenger-Überwachung.

[4] Der Spiegel, 18.07.2021: *Ungarische Regierungsgegner und Journalisten wurden offenbar ausgespäht.* Online abrufbar unter Cyberwaffe »Pegasus«: Journalisten in Ungarn sollen ausgespäht worden sein - DER SPIEGEL.

[5] Der Spiegel, 17.04.2024: Polnische PiS-Regierung hat Pegasus wohl hundertfach im eigenen Land eingesetzt. Online abrufbar unter Polen: PiS-Regierung setzte israelische Spionagesoftware Pegasus wohl hundertfach ein - DER SPIEGEL.

nicht in Eigenentwicklung herstellt, wird diese voraussichtlich von externen Anbietern – etwa ausländischen Staaten oder privaten Unternehmen – bezogen.

In solchen Fällen besteht regelmäßig kein Zugang zum Quellcode, weil Anbieter sich auf den Schutz ihrer Geschäfts- und Betriebsgeheimnisse berufen. Die Software wird daher meist in kompilierter Form oder als Dienstleistung („Malware-as-a-Service“) bereitgestellt, wodurch eine unabhängige technische Überprüfung der eingesetzten Technologie faktisch ausgeschlossen ist. Die DSN müsste sich somit allein auf vertragliche Zusicherungen des Anbieters verlassen, ohne sicher feststellen zu können, ob die Überwachungssoftware ausschließlich im rechtlich zulässigen Umfang tätig wird oder gegebenenfalls darüber hinaus Daten ausliest oder an Dritte übermittelt.

Vor diesem Hintergrund erscheint eine gesetzliche Nachschärfung erforderlich. Es sollte unmissverständlich klargestellt werden, dass der Einsatz einer staatlichen Überwachungssoftware nur dann zulässig ist, wenn – nach Abwägung aller Umstände und nach unabhängiger technischer Prüfung – kein begründeter Zweifel daran besteht, dass die Software ausschließlich innerhalb des vorgegeben Rechtsrahmens zum Einsatz kommt. Ein bloßes Vertrauen auf vertragliche Zusagen des Anbieters kann unter diesen Voraussetzungen nicht ausreichend sein.

Durch den Einsatz einer Überwachungssoftware kommt der Staat in einen Interessenkonflikt

Der Entwurf ermächtigt die DSN gemäß § 11 Abs 1 Z 9 SNG eine Schadsoftware in das Computersystem der betroffenen Person einzuschleusen, um auf verschlüsselte Kommunikationsinhalte zugreifen zu können. Voraussetzung für die Installation einer solchen Überwachungssoftware ist das Vorhandensein einer Sicherheitslücke im System der überwachten Person, etwa im Betriebssystem des Endgeräts oder in konkreten Anwendungen. Diese Sicherheitslücke darf nur dem Entwickler der Überwachungssoftware, nicht aber dem Anbieter des Betriebssystems/der Software bekannt sein, weil letztere die Lücke ansonsten beheben würden und die Überwachungssoftware nicht mehr einsatzfähig wäre. Damit wird jedoch nicht nur das Zielsystem, sondern potenziell die gesamte digitale Infrastruktur gefährdet. Gelangt diese Lücke in falsche Hände – etwa durch einen Hackerangriff – könnten auch Kriminelle oder internationale Akteure sie für ihre Zwecke nutzen. Diese unterliegen dann aber freilich nicht jenen strengen Einschränkungen, die im Entwurf für den Einsatz durch die DSN vorgesehen sind. Medienberichten zufolge ist dies auch bereits tatsächlich passiert.[6]

Hieraus resultiert ein gravierender Interessenkonflikt des Staates: Einerseits verfolgt der Staat das legitime Ziel, die Cybersicherheit durch gesetzliche Vorgaben, wie etwa das NIS-2-Gesetz,

[6] Der Standard, 1.09.2024: *Die Tricks des „Bundestrojaners“ sind in die Hände Moskaus gefallen*. Online abrufbar unter https://www.derstandard.at/story/3000000234720/die-tricks-des-bundestrojaners-sind-in-die-haende-moskaus-gefallen.

zu gewährleisten. Andererseits ist der Staat für den Einsatz der Überwachungssoftware jedoch auf die Existenz spezifischer Sicherheitslücken angewiesen, wodurch ein direkt entgegengesetztes Interesse entsteht – nämlich, dass diese Lücken nicht geschlossen werden. Ein vergleichbares Spannungsverhältnis zeigt sich auch im Zusammenhang mit Art. 32 des Data Act, weil die darin vorgesehenen Schutzmaßnahmen – insbesondere zum Schutz vor unrechtmäßigem staatlichen Zugriff auf nicht-personenbezogene Daten – grundsätzlich kaum wirksam getroffen werden können, solange ein nicht ausreichend kontrollierter staatlicher Zugang möglich ist. Dieser Interessenskonflikt spitzt sich dabei gerade im Bundesministerium für Inneres zu, wo mit der DSN eine einzige Stelle zugleich für die Gewährleistung der Cybersicherheit und die Durchführung staatlicher Überwachungsmaßnahmen zuständig ist.

Unklare Mitwirkungspflicht der Telekommunikationsbetreiber

Für die Überwachung unverschlüsselter wie auch verschlüsselter Nachrichten wird die DSN in der Praxis auf die Mitwirkung privater Telekommunikationsbetreiber angewiesen sein, die für die überwachte Person Kommunikationsinfrastruktur oder entsprechende Dienste bereitstellen. Für diese sieht der Entwurf Mitwirkungs- und Auskunftspflichten vor, lässt deren genaue Ausgestaltung aber teilweise offen.

Im Zentrum dieser Bedenken steht die im Entwurf enthaltene – jedoch nicht näher definierte – Verpflichtung der Betreiber, bei der „eindeutigen Zuordnung eines Computersystems des Betroffenen“ mitzuwirken. Diese Formulierung ist als Legaldefinition unzureichend und schafft keine Rechtssicherheit betreffend des Umfangs der geforderten Mitwirkungspflichten.

Je nach Ausgestaltung der Mitwirkungspflichten wären gegebenenfalls Investitionen erforderlich, die nach der Investitionskostenersatzverordnung (IKEV 2023) abgegolten werden müssen. Damit der Kostenersatz geltend gemacht werden kann, wären die entsprechenden Bestimmungen in ÜKVO, IKEV 2023 und TKG auch um Verweise auf die Verpflichtung nach dem SNG zu ergänzen.

<u>Fehlende Ermächtigungsgrundlage zur Übermittlung von Verkehrsdaten</u>

Im Rahmen des vorliegenden Entwurfs sind Änderungen der §§ 161 ff TKG vorgesehen, die in § 162 Abs 2 TKG nunmehr explizit eine Mitwirkungspflicht der Betreiber bei der eindeutigen Zuordnung von Computersystemen normieren. Bei der Erhebung solcher Daten handelt es sich jedoch um Verkehrsdaten im rechtlichen Sinne. Das Fehlen einer ausdrücklichen gesetzlichen Ermächtigungsgrundlage für die Übermittlung solcher Verkehrsdaten – etwa zur technischen Zuordnung eines Endgeräts durch die dynamische IP-Adresse – führt dazu, dass die Beauskunftung von Verkehrsdaten in diesen Fällen rechtlich unzulässig ist. Denn gemäß § 167 Abs 5 TKG ist die Auskunftserteilung über Verkehrsdaten nur in den ausdrücklich gesetzlich vorgesehenen Ausnahmefällen zulässig. Der Anwendungsbereich des § 11 Abs 1 Z 9 SNG wird von den abschließend aufgezählten Ausnahmebestimmungen des TKG jedoch nicht erfasst. Mangels einer klaren gesetzlichen

Grundlage ist es den betroffenen Anbietern daher derzeit nicht möglich, die erforderlichen Verkehrsdaten zur Gerätezuordnung zu übermitteln. Eine Verpflichtung zur Mitwirkung ohne eine entsprechende gesetzliche Ermächtigung würde nicht nur dem Legalitätsprinzip widersprechen, sondern die Betreiber auch einem erheblichen haftungs- und datenschutzrechtlichen Risiko aussetzen. Die bloße Übermittlung von Stammdaten ist zur Umsetzung der geforderten Zuordnung nicht ausreichend, weil diese in der Regel keine Rückschlüsse auf das konkret verwendete Computersystem oder die eingesetzte Hardware zulassen.

Die ISPA begrüßt ausdrücklich, dass der Entwurf keine aktive Mitwirkungspflicht der Betreiber in Form gezielter technischer Eingriffe – etwa die Zuweisung fixer IP-Adressen – vorsieht. Gleichwohl bedarf es einer gesetzlich klar geregelten und verfassungskonformen Grundlage, die Inhalt, Umfang und Grenzen etwaiger Mitwirkungspflichten konkret bestimmt und sowohl dem Prinzip der Verhältnismäßigkeit als auch den Anforderungen an Rechtssicherheit genügt.

Begriff des Computersystems zu weit gefasst

Hinsichtlich der im Entwurf vorgesehenen Maßnahme nach § 11 Abs 1 Z 9 SNG bestehen über den technischen Anwendungsbereich hinaus auch begriffliche Unklarheiten, die einer gesetzlichen Präzisierung bedürfen. Dies betrifft insbesondere die Verwendung des Begriffs „Computersystem“, der für die Reichweite der Eingriffsbefugnis entscheidend ist.

Gemäß § 74 Abs 1 Z 8 StGB umfasst ein „Computersystem“ sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen. Vom Wortlaut her ist damit nicht zwingend eine physische Verfügungsgewalt der betroffenen Person über das jeweilige System erforderlich. Es ist daher nicht ausgeschlossen, dass auch von Dritten betriebene, aber vom Betroffenen genutzte Cloud-Dienste unter diesen Begriff fallen. Ein Zugriff auf derartige externe Systeme würde jedoch erhebliche Sicherheitsrisiken für die Anbieter sowie für sämtliche weitere Nutzer:innen dieser Dienste mit sich bringen. Der Gesetzgeber sollte daher ausdrücklich klarstellen, dass ein Zugriff auf Cloud-Infrastrukturen Dritter nicht von der Eingriffsbefugnis erfasst ist. Gleiches gilt für die in den Erläuterungen enthaltene Formulierung, wonach die Maßnahme auch „andere Geräte, die eine Internetverbindung ermöglichen“ betreffen soll. Diese Formulierung ist insofern problematisch, weil sie potenziell auch den Zugriff auf Smart-Home-Systeme, vernetzte Haushaltsgeräte oder andere IoT-Komponenten einschließen könnte. Eine derart weitreichende Eingriffsmöglichkeit ist nicht nur aus grundrechtlicher, sondern auch aus sicherheitstechnischer Sicht bedenklich und sollte durch eine einschränkende gesetzliche Auslegung ausgeschlossen werden.

Erleichterter Zugriff auf Inhaltsdaten und mögliche unbegrenzte Ausleitung von Internetdatenverkehr

Mit den geplanten Änderungen des § 11 Abs 1 Z 8 SNG wird es nunmehr ermöglicht, im Bereich der Gefahrenabwehr eine Internetdatenüberwachung anzuordnen. Durch die Integration des erweiterten Begriffs „Informationen“ in das SNG wird eine rechtliche Grundlage

geschaffen, die künftig auch die Überwachung von Internetdatenverkehr im Rahmen der sogenannten Packet-Switched Interception (PSI) ermöglicht.

Eine solche Änderung würde jedoch eine Anpassung der Überwachungsverordnung (ÜVO) erfordern. Da die ÜVO jedoch lediglich die technischen Standards für die Überwachung festlegt, ohne zwischen den Behörden zu unterscheiden, die eine Ausleitung von IP-Inhalten anordnen können, wäre es künftig möglich, dass nicht nur im Rahmen des SNG, sondern auch auf Antrag anderer Behörden, wie etwa der Strafverfolgungsbehörden, eine Ausleitung von Internetdatenverkehr erfolgen könnte. Darüber hinaus könnte die Erweiterung der Befugnisse auf weitere Behörden eine unangemessene Beeinträchtigung der Grundrechte betroffener Personen nach sich ziehen und die rechtsstaatlichen Prinzipien, die den Schutz individueller Freiheiten garantieren, gefährden. Zudem bestünde eine erhöhtes Missbrauchspotenzial, das eine flächendeckende Internetdatenüberwachung betroffener Personen zur Folge haben könnte, die künftig auch von anderen Behörden als der DSN angefordert werden könnte.

Die ISPA lehnt eine derart weitreichende Überwachung entschieden ab. Sollte eine solche Maßnahme dennoch in Betracht gezogen und umgesetzt werden, muss ausdrücklich geregelt werden, dass die Ausleitung von IP-Inhalten ausschließlich auf Grundlage des SNG erfolgen kann und nicht auch von anderen Strafverfolgungsbehörden angeordnet werden darf, wobei es zudem notwendig ist, dass sämtliche Anordnungen nach § 11 Abs 1 Z 8 SNG dokumentiert und statistisch erfasst werden, um ein Mindestmaß an Transparenz, Kontrolle und öffentlicher Nachvollziehbarkeit zu gewährleisten.

Erweiterung technischer Überwachungsmaßnahmen durch IMSI- und WLAN-Catcher

Die im Entwurf vorgesehenen Ermittlungsmaßnahmen gemäß § 11 Abs 1 Z 5 und Z 7 SNG betreffen den möglichen Einsatz von IMSI- und WLAN-Catchern zur Ermittlung von Standort- und Verkehrsdaten ohne Mitwirkung der Telekommunikationsbetreiber. Hierfür sollen Geräte wie IMSI-Catcher zum Einsatz gelangen, die ein Mobilfunknetz beziehungsweise eine Basisstation simulieren und sämtliche Mobiltelefone im Umkreis zur Verbindung zwingen. Auch bei WLAN-Catchern besteht eine vergleichbare Funktionalität für den WLAN-Funkverkehr.

Der Einsatz dieser Geräte ist aus Sicht der ISPA jedoch äußerst bedenklich: Er führt unweigerlich zur Erfassung der Daten sämtlicher Endgeräte, die sich im Einzugsbereich befinden – also auch von Personen, gegen die keinerlei Verdacht im Sinne des § 6 SNG besteht. Dies stellt einen erheblichen Eingriff in das Recht auf Achtung des Privatlebens (Art. 8 EMRK) dar und erweitert die Überwachungsmaßnahmen nicht nur auf Kontakt- und Begleitpersonen, sondern auch auf Personen, die sich lediglich geografisch im selben Bereich aufhalten. Das Fehlen technischer und organisatorischer Schutzvorkehrungen im Gesetz schließt potenzielle Missbrauchsmöglichkeiten weder aus noch ermöglicht es eine wirksame Kontrolle oder Begrenzung. Zudem sieht das Gesetz keine nachträgliche Information der betroffenen, unbeteiligten Personen vor.

Technische Studien zeigend darüber hinaus, dass der Einsatz von IMSI-Catchern nicht nur datenschutzrechtlich, sondern auch funktional bedenklich ist. So kann es etwa durch Netzüberlagerungen zu Störungen des Mobilfunkverkehrs kommen, wodurch für einen begrenzten Zeitraum auch keine Notrufe abgesetzt werden können. Netzbetreiber befürchten, dass eine durch den Einsatz eines IMSI-Catchers verursachte Störung deutlich länger andauern könnte als der Zeitraum, der für die Erfassung einer einzelnen IMSI erforderlich ist. Laut dem Hersteller Rohde & Schwarz kann im Einzugsbereich des IMSI-Catchers während des gesamten Einschaltzeitraums – der voraussichtlich zwischen 5 und 10 Minuten liegt – kein Gespräch aufgebaut und somit auch kein Notruf abgesetzt werden.[7] Dies stellt ein erhebliches sicherheits- und gesundheitspolitisches Risiko dar.

Potenzielle Einführung einer Vorratsdatenspeicherung

Die geplanten Änderungen des § 53 Abs 3b SPG geben Anlass zur Kritik: Mit dem Entfall der Kurzbezeichnung „IMSI“ soll klargestellt werden, dass nicht nur die klassische „International Mobile Subscriber Identity“, sondern etwa auch der im 5G-Netz verwendete „Subscription Permanent Identifier (SUPI)“ erfasst ist. Damit wird der Anwendungsbereich technischer Überwachungsmaßnahmen erheblich ausgeweitet. Eine solche Vorgehensweise ist jedoch derzeit nicht durch eine entsprechende Verordnungsermächtigung im TKG gedeckt, weil die bestehenden Regelungen der Strafprozessordnung (StPO) keine Mitwirkungspflicht der Betreiber vorsehen. Sollte eine solche Mitwirkung jedoch erforderlich sein, bedarf es einer entsprechenden Änderung der Überwachungsverordnung (ÜVO).

Besonders kritisch erachtet die ISPA in diesem Zusammenhang die Möglichkeit, dass durch den Einsatz entsprechender Geräte Kommunikations- oder Standortdaten – selbst nur kurzfristig – lokal zwischengespeichert oder „gecached“ werden. Eine derartige Datenverarbeitung stellt der Systematik nach eine Vorratsdatenspeicherung dar. Diese ist im geltenden Recht ausdrücklich nicht vorgesehen und entbehrt daher jeglicher gesetzlichen Grundlage. Hinzu kommt, dass erhebliche Zweifel bestehen, ob ein solches Vorgehen mit den Vorgaben des EU-Rechts, in Einklang steht.

Wertungswiderspruch durch Backup-Überwachung

Die im Entwurf vorgesehene Überwachung durch eine staatliche Überwachungssoftware gemäß § 11 Abs 1 Z 9 SNG bezieht sich explizit auf Nachrichten, also auf Kommunikationsvorgänge. Auch aus den Erläuterungen zum Ministerialentwurf geht hervor, dass eine Durchsuchung des gesamten Computersystems, einschließlich lokal gespeicherter Daten, ausgeschlossen ist. Jedoch wird in den Erläuterungen klargestellt, dass nicht nur Nachrichten, die über internetbasierte Kommunikationsdienste wie WhatsApp oder Telegram übermittelt werden, erfasst sind, sondern auch Datenpakete, die von einem Cloud-Diensteanbieter an einen Cloud-Server übermittelt werden. Dies wirft die Frage auf, ob auch

[7] Researchgate: Der IMSI_catcher. Online abrufbar unter https://www.researchgate.net/publication/220174414_Der_IMSI-Catcher

Geräte-Backups, die an einem Backup-Server übertragen werden, unter die Überwachung fallen.

Damit wäre es für die Ermittler zwar einerseits unzulässig, die lokal am Endgerät gespeicherten Daten (wie unter anderem gespeicherte Standortdaten, Notizen, Bilder, Musik, Videos, Gesundheitsdaten von Wearables etc.) mittels der Überwachungssoftware auszulesen, sobald diese Dateien aber in Form eines Backups an einen Server übermittelt werden, wäre der Zugriff darauf auf einmal rechtlich unproblematisch. Da diese Daten typischerweise erheblich umfangreicher und teils auch sensibler sind als diejenigen, die über bloße Chats übermittelt werden, sollte die Legitimität des Zugriffs durch Ermittlungsbehörden nicht davon abhängen, ob die überwachte Person die Backupfunktion auf dem Telefon aktiviert hat.

Streichung der Überwachung von M2M-Kommunikation

In den Erläuterungen des Entwurfs wird nun ausdrücklich vorgesehen, dass die M2M-Kommunikation (Machine-to-Machine-Kommunikation) vom Anwendungsbereich der Überwachungsbefugnisse erfasst werden soll. Diese Erweiterung führt zu erheblichen Abweichungen im Vergleich zu der bisherigen Regelung des § 134 Z 3 StPO, die ausschließlich die Kommunikation zwischen natürlichen Personen erfasst. Die Einbeziehung von M2M-Kommunikation stellt nicht nur eine erhebliche technische Herausforderung dar, sondern ist auch mit hohen Investitionskosten für die Telekommunikationsbetreiber verbunden, die hierfür entsprechende Überwachungstechnik bereitstellen müssten.

Die ISPA fordert daher eine analoge Anwendung zu den bestehenden Regelungen der StPO, die sich klar auf die Kommunikation zwischen natürlichen Personen beziehen, sowie die Streichung des Begriffs „M2M-Kommunikation“ aus dem Entwurf, um einer unverhältnismäßigen und praktisch schwer umsetzbaren Erweiterung der Überwachungsbefugnisse entgegenzuwirken.

II. Grundrechtliche Bedenken

Vorweg ist festzuhalten, dass nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) jede Form der Überwachung geschützter elektronischer Individualkommunikation einen Eingriff in das Recht auf Achtung der Korrespondenz gemäß Art. 8 EMRK darstellt.[8] Solche Eingriffe sind nur dann zulässig, wenn sie auf einer gesetzlichen Grundlage beruhen, der Verfolgung eines legitimen Ziels in einer demokratischen Gesellschaft dienen, einer Verhältnismäßigkeitsprüfung standhalten und das gelindeste zur Verfügung stehende Mittel darstellen.

Gerade bei verdeckten staatlichen Überwachungsmaßnahmen gelten besonders hohe Anforderungen an die rechtliche Bestimmtheit und Vorhersehbarkeit der zugrundeliegenden

[8] EGMR, 14.3.2013, Bernh Larsen Holding AS u.a. / Norwegen, Z. 105 ; VfSlg 20.356/2019 Rn 171

Norm. Darüber hinaus müssen effektive und angemessene Schutzmechanismen gegen möglichen Missbrauch gewährleistet werden. Nach ständiger Rechtsprechung des EGMR sind Maßnahmen systematischer und verdeckter Überwachung zudem einer unabhängigen – in der Regel gerichtlichen – Kontrolle zu unterstellen, um die Rechte der betroffenen Personen wirksam zu schützen.[9]

Rechtlich Nachrichtenüberwachung – faktisch eine Online-Durchsuchung

Der vorliegende Gesetzesentwurf beruht auf einer rechtlichen Unterscheidung, die in der technischen Realität nicht aufrechterhalten werden kann. Er sieht vor, ausschließlich verschlüsselte Kommunikation zu überwachen, ohne dabei eine vollständige Online-Durchsuchung durchzuführen. Technisch ist dies jedoch nicht realisierbar: Der Zugriff auf Nachrichteninhalte über Messenger-Dienste erfordert zwangsläufig einen umfassenden Zugriff auf das gesamte Endgerät.

Damit die Überwachungssoftware überhaupt in der Lage ist, verschlüsselte Nachrichten mitzulesen, muss sie tief in das Betriebssystem eingreifen – mit denselben Rechten wie ein Administrator. Das bedeutet, dass nicht nur Kommunikationsinhalte, sondern auch Fotos, Standortdaten, Dokumente und andere persönliche Informationen zugänglich werden.

Eine klare Trennung zwischen Kommunikationsüberwachung und Online-Durchsuchung ist daher technisch nicht möglich. Auch wenn der Entwurf die Durchführung einer Online-Durchsuchung formal ausschließt, schafft er durch die gewählten technischen Mittel und die weite Auslegung zentraler Begriffe die Voraussetzungen für genau eine solche Maßnahme. Bei der Abwägung mit den betroffenen Grundrechten – insbesondere dem Recht auf Datenschutz gemäß § 1 DSG sowie dem Recht auf Achtung des Privat- und Familienlebens gemäß Art. 8 EMRK – muss dieser Umstand angemessen berücksichtigt werden.

Ausweitung der Überwachung – Von der Strafverfolgung zur Gefahrenabwehr

Der Entwurf sieht vor, dass der Einsatz staatlicher Überwachungstechnologien nunmehr im Bereich der sicherheitspolizeilichen Gefahrenabwehr zur Anwendung kommen soll, konkret zur Abwehr verfassungsgefährdender Bedrohungen. Damit kann die Maßnahme künftig bereits gegen sogenannte „Gefährder“ eingesetzt werden, also Personen, die noch keiner konkreten Straftat verdächtig sind, von denen aber nach Einschätzung der Behörden eine erhebliche Gefahr für die öffentliche Sicherheit ausgeht. Zu beachten ist, dass betroffene Personen in diesem Verfahrensstadium noch nicht als konkret tatverdächtig bzw. Beschuldigte gelten. Ihnen stehen somit auch keine strafprozessualen Verteidigungsrechte zu.

Ein weiterer Aspekt, der im aktuellen Entwurf noch nicht ausreichend adressiert wird, ist das Fehlen einer expliziten Rechtsgrundlage für die Beschwerdemöglichkeit der von der

[9] EGMR, 8.4.2014, Blaj / Rumänien, Z. 128, 133; EGMR Klass u.a. / Deutschland Z 48ff; VfSlg 20.356/2019 Rn 171

Überwachung betroffenen Person. Zwar wird in den Erläuterungen auf § 90 SPG verwiesen, also auf die allgemeine Möglichkeit einer Datenschutzbeschwerde. Betroffene könnten auch gemäß § 88 Abs 2 SPG eine Beschwerde wegen der Verletzung ihrer subjektiven Rechte erheben, wenn sie sich durch die Modalitäten der Ermittlungsmaßnahme in ihren Rechten verletzt fühlen. Für einen effektiven Rechtsschutz ist jedoch anzumerken, dass kein spezifisch auf die Besonderheiten der Überwachungsmaßnahme abgestimmtes Beschwerdeverfahren vorgesehen ist. Dies führt dazu, dass die betroffenen Personen nicht adäquat in ihren Rechten geschützt werden.

Begleitende Kontrolle durch den Rechtsschutzbeauftragten

Der neue Gesetzesentwurf enthält erfreulicherweise einige signifikante Verbesserungen im Bereich der begleitenden Kontrolle. Besonders hervorzuheben ist, dass der Rechtsschutzbeauftragte gemäß § 15c SNG nun erweiterte Kontroll- und Eingriffsrechte erhält. So kann er im Falle einer Bewilligung durch das Bundesverwaltungsgericht Revision beim Verwaltungsgerichtshof einlegen. Des Weiteren wird ihm das Recht eingeräumt, jederzeit Einsicht in nachrichtendienstlich erhobene Daten zu nehmen und diese gegebenenfalls anzuhören. Falls die Daten unzulässig erhoben wurden, kann er deren Löschung verlangen und sich persönlich von der ordnungsgemäßen Durchführung der Löschung überzeugen. Sollte er Zweifel an der Verhältnismäßigkeit einer Maßnahme haben, ist er verpflichtet, beim Bundesverwaltungsgericht die Aufhebung der Bewilligung zu beantragen. In einem solchen Fall muss auch die betroffene Direktion informiert werden, die ein Äußerungsrecht im Verfahren hat. Eine Revision durch den Bundesminister für Inneres gegen eine solche Aufhebung ist ausdrücklich ausgeschlossen. Diese Erweiterung der Kontrollbefugnisse stellt eine längst überfällige und begrüßenswerte Verbesserung dar.

Eine effektive Kontrolle erfordert jedoch mehr als nur juristisches Fachwissen. Sie setzt ein tiefgehendes Verständnis der eingesetzten technischen Mittel voraus. Der Zugriff auf IT-Systeme, der Einsatz von Schadsoftware und die Umgehung von Verschlüsselungstechnologien sind hochkomplexe Vorgänge, die ohne entsprechende technische Expertise nicht vollständig überprüfbar sind. Eine effektive Kontrolle kann daher nur gewährleistet werden, wenn auch IT-Fachkräfte mit entsprechender Expertise in die Überprüfungsprozesse eingebunden sind. Aus diesem Grund regen wir die Einrichtung eines interdisziplinären Rechtsschutzsenats an, der sowohl mit Juristen als auch mit qualifizierten IT-Experten besetzt ist. Nur auf diese Weise kann sichergestellt werden, dass die Überwachungsmaßnahmen nicht nur aus rechtlicher, sondern auch aus technischer Perspektive sachgerecht überprüft werden.

Neu eingeführte Berichtspflicht nach § 17 Abs 3a SNG

Positiv hervorzuheben ist die Einführung einer neuen Berichtspflicht in § 17 Abs 3a SNG: Überschreitet die Anzahl der angeordneten Überwachungsmaßnahmen in einem Kalenderjahr den Schwellenwert von 35, unterliegt der Bundesminister für Inneres einer Berichtspflicht.

Diese Maßnahme stellt einen wichtigen ersten Schritt in Richtung mehr Transparenz dar. Allerdings sieht der Entwurf weder Sanktionen bei unterlassener oder fehlerhafter Berichterstattung noch eine systematische Überprüfung der Berichtspflicht durch unabhängige Stellen vor. Ohne entsprechende Kontrollmechanismen bleibt die Berichtspflicht letztlich ein zahnloses Instrument, das kaum dazu geeignet ist, eine wirksame Transparenz oder Verantwortlichkeit sicherzustellen. Damit wird zwar ein gewisses Maß an institutioneller Kontrolle eingeführt, das grundsätzlich geeignet ist, der Gefahr einer verdeckten Massenüberwachung entgegenzuwirken. Allerdings stellt es in dieser Ausgestaltung kein ausreichend effektives Mittel dar.

Unzureichender Schutz von Berufsgeheimnisträger:innen

Zwar sieht der Entwurf vor, dass Eingriffe in die durch § 157 Abs 1 Z 2 bis Z 4 StPO geschützte berufliche Kommunikation – insbesondere von Rechtsanwält:innen und Journalist:innen – grundsätzlich unzulässig sind. Allerdings fehlt es an verbindlichen verfahrensrechtlichen Vorgaben, die diesen Schutz wirksam und nachvollziehbar gewährleisten. Dabei unterliegt die Kommunikation dieser Berufsgruppen aufgrund ihrer verfassungsrechtlich geschützten Funktion im Rechtsstaat einer besonderen Vertraulichkeit. Eine (auch nur mittelbare) Erfassung dieser Kommunikation durch staatliche Überwachungsmaßnahmen birgt das erhebliche Risiko, grundlegende rechtsstaatliche Prinzipien – wie die das Recht auf eine faire Verteidigung oder den Quellenschutz – nachhaltig zu gefährden. Umso dringlicher ist es, den Schutz dieser Berufsgruppen durch präzise verfahrensrechtliche Bestimmungen normativ abzusichern.

So sehr der Gesetzesentwurf in einzelnen Aspekten begrüßenswerte Fortschritte erkennen lässt, bestehen weiterhin erhebliche Bedenken hinsichtlich der grundrechtlichen Eingriffe sowie der technischen Umsetzbarkeit der rechtlichen Vorgaben und der Gewährleistung einer wirksamen Kontrolle. Die vorgesehene Ausgestaltung erscheint in ihrer derzeitigen Form nicht geeignet, eine wirksame Kontrolle sicherzustellen. Auch wenn die ISPA die Strafverfolgungsbehörden im Vollzug ihrer Aufgaben grundsätzlich unterstützt und einer effektiven sowie vertrauensvollen Zusammenarbeit zur Wahrung der öffentlichen Sicherheit offen gegenübersteht, setzt dies voraus, dass die Grundrechte gewahrt und unabhängige Kontrollmechanismen verlässlich sichergestellt werden.

Mit freundlichen Grüßen,

Mag. Stefan Ebenberger

Generalsekretär ISPA

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675
DVR-Nr.: 0931977

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675
DVR-Nr.: 0931977