Messengerdienste: Darf der Staat bald mitlesen?
Philipp Fellinger & Annette GantnerWIEN/ Linz.

(Oberösterreichische Nachrichten, 08.04.2025, Seite 3=

Die Regierungsklausur startet heute mit dem Thema Sicherheit. Am Montag liefen die Verhandlungen zur Überwachung der Messengerdienste auf Hochtouren, doch es spießte sich an mehreren Details. ÖVP, SPÖ und Neos haben sich im Regierungsübereinkommen auf eine verfassungskonforme Gefährderüberwachung, wie sie nun zunehmend bezeichnet wird, geeinigt. Vor allem die Neos pochen hier auf eine rechtlich saubere Lösung.Die OÖNachrichten liefern einen Überblick über die Vorteile der Messengerüberwachung und über die Sorgen vor einem zu starken Zugriff des Staates auf private Daten.Warum wird eine Messengerüberwachung gefordert? Terroristen haben ihre Kommunikationsmethoden dem digitalen Zeitalter angepasst. Attentatsplanungen finden zu einem Großteil über das Netz statt - und dort vor allem auf sogenannten Messengerdiensten wie Signal, WhatsApp, Telegram oder Facebook-Messenger. Diese verfügen über eine Verschlüsselung, können mit herkömmlichen Methoden nicht ausgelesen werden. Das Innenministerium fordert daher seit Sommer die Möglichkeit, bei "verfassungsgefährdenden Angriffen" eine Überwachungssoftware - auch "Bundestrojaner" genannt - auf Mobiltelefonen von potenziellen Tätern einzuschleusen.Wieso gibt es noch kein entsprechendes Gesetz für eine Messengerüberwachung?Ein Entwurf liegt seit August vor, doch wurde dieser damals vom grünen Koalitionspartner nicht unterstützt. Zu groß waren die Bedenken, dass damit Missbrauch ermöglicht wird. Ein ganz ähnliches Gesetz hatte bereits die Bundesregierung unter VP-Kanzler Sebastian Kurz im Jahr 2018 auf den Weg gebracht. Bereits ein Jahr später hob der Verfassungsgerichtshof (VfGH) dieses aber wieder auf. Warum hob der Verfassungsgerichtshof die Messengerüberwachung bereits einmal auf?Dem VfGH gingen die Berechtigungen für den Einsatz der Software zu weit. Ermittler konnten Geräte zur Gänze, nicht etwa "nur" Chatverläufe sichten. Die Höchstrichter hatten auch andere Einwände: Als unzureichend sahen sie etwa den Rechtsschutz an, also die Kontrolle für den Einsatz von Überwachung. Diese sollte durch ein Gericht oder eine Behörde mit vergleichbarer Unabhängigkeit erfolgen. Als verletzt sah der VfGH vor allem den Artikel 8 der Europäischen Menschenrechtskonvention an. Dieser umfasst das Recht auf Achtung des Privatlebens. Welche Einwände hatten die Experten?Vor allem Datenschützer sehen in dem Entwurf eine Grundrechts- und Datensicherheitsgefährdung. Sebastian Kneidinger von der Organisation "epicenter.works" erkennt in dem Entwurf vom August 2024 keine Verbesserungen zum aufgehobenen Gesetz von 2019: "Die damaligen Einwände werden so gut wie nicht berücksichtigt." Es sei daher nicht unwahrscheinlich, dass auch die neue Version wieder aufgehoben werde. Für Kneidinger sprechen zwei weitere Umstände gegen die Umsetzung: Der Staat muss für die Überwachung Sicherheitslücken auf Mobiltelefonen seiner Bürger verschweigen, das Wissen über Lücken müsste bei halblegalen Anbietern beschafft werden. Ist eine verfassungskonforme Messengerüberwachung überhaupt möglich? Hier treffen verschiedene Meinungen aufeinander. Das Innenministerium beteuert, dass die Spähsoftware verfassungskonform möglich sei. Innenminister Gerhard Karner (VP) spricht davon, dass es nicht um eine Massenüberwachung gehe, betroffen seien 30 bis 50 Fälle pro Jahr. "Faktum ist: Die Bevölkerung ist davon nicht betroffen, es geht um Gefährder und Terroristen", sagte Karner am Sonntag in der ORF-Pressestunde. Ziel müsse sein, Polizei und Verfassungsschutz mit den international üblichen modernen Methoden zur Überwachung von Extremisten und Terroristen auszustatten. "Epicenter.works" verweist genauso wie die Richtervereinigung darauf, dass es technisch überhaupt nicht möglich sei, die Überwachung nur auf einzelne Chatverläufe zu beschränken. Damit wäre es nicht möglich, einen der wesentlichsten vom VfGH festgestellten Mängel zu beheben. Deutschland benutzt seit Jahren einen "Bundestrojaner". Wie funktioniert dieser? Quellen-Telekommunikationsüberwachung (TKÜ) heißt die Messengerüberwachung der

deutschen Behörden. Die Software dringt auf das Mobiltelefon eines Verdächtigen ein und ermöglicht den Zugriff auf Messenger-Kommunikation, bevor diese verschlüsselt wird. Bisher unklar ist, ob die Nutzung eines ähnlichen Modells in Österreich verfassungskonform wäre. Hätten mit der Messengerüberwachung Terrorakte verhindert werden können?Hier wird argumentiert, dass etwa der mutmaßliche Terrorist, der ein Attentat auf die Besucher des Taylor-Swift-Konzerts geplant hatte, vorzeitig aus dem Verkehr gezogen hätte werden können und man nicht auf die US-amerikanischen Geheimdienste angewiesen gewesen wäre. Das Attentat von Villach hätte hingegen nicht vermieden werden können. Auch bei den jüngst bekannt gewordenen organisierten Attacken auf Homosexuelle hätte eine Messengerüberwachung keinen Nutzen gehabt. Datenschutzexperte Kneidinger sieht es daher als sinnvoller an, personelle Ressourcen etwa in das Auslesen von Telegram-Gruppen zu stecken. Diese seien öffentlich zugänglich. Welche Positionen vertreten die anderen Parteien? In der Politik wird das Thema seit Jahren kontrovers verhandelt. Bisher war die ÖVP mit ihrer Forderung allein auf weiter Flur. Für die SPÖ signalisierte der Staatssekretär im Innenministerium, Jörg Leichtfried, Zustimmung. Die Neos meldeten Bedenken an. Sie wollen nur zustimmen, wenn die Lösung verfassungskonform ist. Vor allem die Möglichkeit, alle Daten auszulesen, bereitet dem dritten Koalitionspartner Kopfzerbrechen. Dieser fordert daher, dass nur Messenger-Nachrichten erfasst werden. Ähnlich ist die Position der Grünen. Die FPÖ ist seit einiger Zeit strikt gegen die Messengerüberwachung, sie sieht darin die Gefahr einer "Massenüberwachung".