166 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVIII. GP

Bericht

des Ausschusses für innere Angelegenheiten

über den Antrag 210/A(E) der Abgeordneten Süleyman Zorba, Kolleginnen und Kollegen betreffend Nein zu Bundestrojaner und Messenger-Überwachung

Die Abgeordneten Süleyman **Zorba**, Kolleginnen und Kollegen haben den gegenständlichen Entschließungsantrag am 24. April 2025 im Nationalrat eingebracht und wie folgt begründet:

„Am 8. April wurde vom Innenminister ein neuer Entwurf für eine Messenger-Überwachung in Begutachtung geschickt und damit eine langjährige ÖVP-Forderung umgesetzt.[1] Die Idee einer Überwachung von Messenger-Diensten zur Kriminalitätsbekämpfung erscheint vielleicht auf den ersten Blick plausibel – Fakt ist aber, dass die angekündigten durchschlagenden Ermittlungserfolge nicht zu erwarten sind und die behauptete technische Umsetzung zahlreiche und eklatante Sicherheitsprobleme und rechtliche Probleme aufwirft.

1. Missbrauch von Spyware

Die Erfahrungen mit Spyware zur Überwachung verschlüsselter Kommunikation zeigen: Wird Spyware verwendet, ist vorprogrammiert, dass diese Systeme regelwidrig eingesetzt werden. So wurden in den vergangenen Jahren unzählige Skandale aufgedeckt, in denen derartige Systeme gegen Opposition, Journalist:innen und Zivilgesellschaft zum Einsatz gebracht wurden:

- Im Jahr 2021 haben mehrere Organisationen der Zivilgesellschaft und investigative Journalist:innen nach und nach aufgedeckt, dass staatliche Stellen in mehreren Ländern, sowohl in EU-Mitgliedstaaten als auch in Drittländern, Pegasus und ähnliche Überwachungs- und Spähsoftware gegen Journalist:innen, Politiker:innen, Strafverfolgungsbeamt:innen, Diplomat:innen, Rechtsanwält:innen, Geschäftsleute, Akteure der Zivilgesellschaft und andere Personen zu politischen und sogar kriminellen Zwecken eingesetzt hatten. Der Missbrauch erfolgte sowohl von autoritären als auch demokratischen Regierungen. Spuren führten nach Polen, Ungarn, Griechenland, Zypern, Spanien, Niederlande, Belgien, Deutschland, Malta, Frankreich, Irland, Luxemburg, Italien und auch nach Österreich. So nutzten im Juli 2022 Betreiber Spähsoftware des damals in Österreich ansässigen Unternehmens DSIRF, um sich in Anwaltskanzleien, Banken und

1 https://www.parlament.gv.at/gegenstand/XXVIII/ME/8

Beratungsunternehmen in Österreich, Panama und Großbritannien einzuhacken. Das ist das Ergebnis des EU-Untersuchungsausschusses zu der Affäre.[2]

- Die nationalkonservative PiS hat in Polen von 2017 bis 2022 Pegasus eingesetzt, um 578 Personen, darunter Oppositionspolitiker:innen zu überwachen. [3]

- 2022 informierte Citizen Lab, dass mit den Spyware-Produkten Candiru und Pegasus Mitglieder des europäischen Parlaments, Jurist:innen, Aktivist:innen und Catalanische Politiker:innen überwacht wurden. Betroffen waren teilweise auch Familienmitglieder der eigentlichen Zielpersonen.[4]

- 2022 wurden in Griechenland 92 Personen darunter Politiker:innen, Minister:innen und Journalist:innen mit der Predator Software angegriffen.[5]

- 2023 wurden Vertreter:innen der Zivilgesellschaft, Journalist:innen, Vertreter:innen der Vereinten Nationen, die deutsche Botschafterin in den USA sowie Politiker:innen in der Europäischen Union (darunter die Präsidentin des Europäischen Parlaments), den USA und Asien mit der Predator-Spionagesoftware angegriffen.[6]

- Im Februar 2024 wurde bei Mitgliedern und Mitarbeiter:innen des EU-Unterausschusses für Sicherheit und Verteidigung auf Smartphones Überwachungssoftware gefunden.[7]

- von 2023 bis 2025 wurde in Serbien die Spionagesoftware Pegasus gegen Journalist:innen, Umweltaktivist:innen und andere Personen wiederholt eingesetzt.[8]

Das sind nur ein paar der bekannt gewordenen Skandale rund um den Einsatz von Überwachungs-Software, die zeigen: Der Missbrauch ist Überwachungssystemen immanent.

2. Technische Machbarkeit nicht gegeben

In § 15a Abs 3 des Ministerialentwurfs wird geregelt, dass eine Bewilligung nur in jenem Umfang und für jenen künftigen Zeitraum erteilt werden darf, der zur Erfüllung der Aufgabe voraussichtlich erforderlich ist.

---

2 https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_DE.pdf; https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_DE.html; https://netzpolitik.org/2021/pegasus-der-staatstrojaner-skandal-im- https://www.tagesschau.de/ausland/europa/pegasus-bericht-eu-100.html

3 https://www.euractiv.de/section/europa-kompakt/news/abhoerskandal-in-polen-ueber-500-personen-mit-pegasus-software-gehackt/

4 https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ ; mehr über Candiru: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

5 https://www.euractiv.de/section/innovation/news/griechischer-abhoerskandal-eu-sieht-sein-nationale-zustaendigkeit/

6 https://www.amnesty.de/informieren/aktuell/untersuchung-predator-files-angriff-privatsphaere-deutschland

7 https://netzpolitik.org/2024/nach-spyware-fund-im-eu-parlament-buergerrechtsorganisationen-fordern-verbot-von-spionagesoftware/

8 https://www.amnesty.org/en/latest/news/2025/03/serbia-birn-journalists-targeted-with-pegasus-spyware/

§ 15b Abs 1 regelt weiters:

§ 15b. (1) Bei der Durchführung einer Ermittlungsmaßnahme gemäß § 11 Abs. 1 Z 9 ist technisch sicherzustellen, dass

1. ausschließlich innerhalb des Bewilligungsumfangs und -zeitraums (§ 15a Abs. 3) gesendete, übermittelte oder empfangene Nachrichten überwacht werden können,
2. an dem zu überwachenden Computersystem nur Veränderungen vorgenommen werden, die für die Nachrichtenüberwachung unerlässlich sind, und
3. das eingebrachte Programm nach Beendigung der Ermittlungsmaßnahme entfernt oder funktionsunfähig wird.

Insofern deckt sich der Entwurf mit jenem aus August 2024, zu dem es bereits eine Begutachtung gab. In diesem Begutachtungsprozess gab es klare Stellungnahmen von Expert:innen, die offenlegten, dass derartige Beschränkungen technisch nicht umsetzbar sind.

So wird in der Stellungnahme des Instituts für Netzwerke und Sicherheit und des Instituts für Strafrechtswissenschaften an der Johannes Kepler Universität Linz festgehalten, dass es ‚*zutiefst unrealistisch*' sei, dass diese Vorgaben kontrollierbar gehalten werden könnten. Konkret wird ausgeführt: ‚*Aufgrund der erwähnten Komplexität zur Einbringung des Trojaners und Durchführung der Überwachungsmaßnahmen ist unwahrscheinlich, dass die entsprechenden Filter direkt im eingebrachten Programm implementiert werden. Die realistische Variante ist eine Exfiltration bzw. Ausleitung aller Daten der betroffen Ziel-Anwendungen (z.B. Messenger-Dienste), um diese dann am Auswertungssystem entsprechend filtern zu können.* '[9]

Auch auf der Website des österreichischen nationalen CERT (Computer Emergency Response Team) wird ausgeführt wird, dass die technischen Lösungen verschiedenster Anbieter kommerzieller Spyware (auf die wohl zurückgegriffen werden würde, siehe auch Punkt 3) allesamt nicht dafür ausgelegt sind, nur bestimmte Applikationen zu überwachen. Dasselbe gilt für die Anforderung, dass nur Nachrichten innerhalb eines in einer Anordnung festgesetzten Beobachtungszeitraumes überwacht werden dürfen. Auf cert.at wird festgehalten: ‚*Die Kompromittierung eines Endgerätes mit kommerzieller Spyware bedeutet immer, dass die Privatsphäre der betroffenen Personen vollständig kompromittiert ist.*'[10]

Auch dass das Programm nach Beendigung der Überwachung entfernt oder funktionsunfähig wird, ist aus technischer Sicht nicht anzunehmen. So hält die TU Wien fest: ‚*Die Installation einer solchen Software ist in Systemen mit heute üblicher technischer Komplexität nicht reversibel verwirklichbar*.'[11]

3. Woher kommt die Software?

---

9 Stellungnahme von Univ.-Prof. Dr. René Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit, Univ.-Prof. Dr. Alois Birklbauer, Vorstand des Instituts für Strafrechtswissenschaften, Assoc.-Prof. Dr. Michael Sonntag, Stellvertretender Vorstand des Instituts für Netzwerke und Sicherheit an der Johannes Kepler Universität Linz,
https://www.parlament.gv.at/PtWeb/api/s3serv/file/4addf554-1f1b-4a9e-bd54-070f1749e5e5

10 Alle Jahre wieder: Bundestrojaner und Messengerüberwachung
https://www.cert.at/de/blog/2024/8/alle-jahre-wieder-staatstrojaner-und-messengeruberwachung.

11 https://informatics.tuwien.ac.at/news/1223

§ 11 Abs 1 Z 9 spricht sehr kursorisch vom ‚*Einbringen eines Programms in ein Computersystem (§ 74 Abs. 1 Z 8 StGB) eines Betroffenen […] unter Einsatz technischer Mittel*'.

Diese völlig unbestimmte Formulierung lässt offen, wie dieses ‚Einbringen' tatsächlich erfolgen soll. Voraussetzung wäre eine vorsätzliche Umgehung von Betriebssystem-Sicherheitsmaßnahmen, die ja gerade darauf abzielen, Endgeräte vor Zugriffen von außen zu schützen. Das bedeutet, dass sowohl beim ‚Einbringen' als auch beim Betrieb der Überwachungsmaßnahmen (noch) offene Sicherheitslücken aktiv ausgenützt werden müssten. Da es sich hier um ein sich ständig veränderndes System handelt, ist die Komplexität so eines Angriffs gegen Sicherheitsmaßnahmen sehr hoch.

Insofern ist es völlig unwahrscheinlich, dass österreichische Sicherheitsbehörden die Ressourcen haben, um selbst die sich stetig ändernden Sicherheitslücken zu identifizieren. Vielmehr wird hier ein Zukauf existierender Spyware erfolgen. Derartige Spyware sieht aber wiederum keine Beschränkungen vor, wie sie das Gesetz in seinen §§ 15a und 15b regelt bzw würde man sich dann auf freundliche ‚Zusicherungen' von Spyware-Herstellern verlassen müssen. Nicht zuletzt wäre der Einsatz so einer zugekauften Spyware auch aus datenschutzrechtlicher Sicht in höchstem Maß bedenklich und würde den in Sonntagsreden propagierten Plänen, eine digitale Souveränität herzustellen, diametral zuwiderlaufen.

Generell widerspricht der Zukauf von Spyware auch den allgemeinen Zielen, die IT-Sicherheit zu stärken. Im soeben präsentierten Deloitte Cyber Security Report 2025 zeigt sich, dass Cyber-Angreifer immer aggressiver und erfolgreicher werden.[12] Bestehende Sicherheitslücken sind somit ein enormes Sicherheitsrisiko – und keine Anstrengungen zu unternehmen, sie zu schließen ist ein klarer Widerspruch zu den Anforderungen der NIS2-Richtlinie.[13] So wird Kriminalitätsbekämpfung zur Kriminalitätsbeförderung.

4. Problematisches Ausnützen von Sicherheitsschwachstellen

Schon zum Bundestrojaner 1 hat der Fakultätsrat der TU Wien festgehalten, dass die Ausnutzung von Sicherheitsschwachstellen am Zielsystem den Staat in einen Interessenkonflikt bringt: ‚*Der Staat muss als Folge dieses Gesetzes an der Geheimhaltung der Sicherheits-Schwachstellen in Computersystemen interessiert sein, während er gleichzeitig, beispielsweise in der »Österreichischen Strategie für Cyber Sicherheit«, explizit ein gegenteiliges Interesse verfolgt.* '[14]

Auch im neuen Bundestrojaner-Entwurf stellt sich dasselbe Problem. Grundsätzlich trifft den Staat eine Schutzpflicht: Sowohl Art 8 EMRK als auch Art 10a StGG verpflichten den Staat, die Unverletzlichkeit der Individualkommunikation gegen Gefahren zu schützen.

---

12 https://www.deloitte.com/at/de/services/risk-advisory/research/deloitte-cyber-security-report.html
13 cert.at, Alle Jahre wieder: Bundestrojaner und Messengerüberwachung
https://www.cert.at/de/blog/2024/8/alle-jahre-wieder-staatstrojaner-und-messengeruberwachung,
Stellungnahme von Univ.-Prof. Dr. René Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit, Univ.-Prof. Dr. Alois Birklbauer, Vorstand des Instituts für Strafrechtswissenschaften, Assoc.-Prof. Dr. Michael Sonntag, Stellvertretender Vorstand des Instituts für Netzwerke und Sicherheit an der Johannes Kepler Universität Linz,
https://www.parlament.gv.at/PtWeb/api/s3serv/file/4addf554-1f1b-4a9e-bd54-070f1749e5e5;
Stellungnahme des Chaos Computer Club Wien,
https://www.parlament.gv.at/PtWeb/api/s3serv/file/4caea140-0da6-43a8-9bbe-b5f6f73224ce
14 https://informatics.tuwien.ac.at/news/1223

Das bewusste In-Kauf-Nehmen von Sicherheitslücken, ohne die eine Überwachung im Rahmen eines Bundestrojaners unmöglich wäre, steht in diametralem Widerspruch zu dieser positiven Schutzpflicht.

Derartige Sicherheitslücken existieren nicht nur in den Endgeräten Verdächtiger sondern in den Endgeräten aller Bürger:innen, in den Endgeräten von Unternehmen, Gebietskörperschaften und öffentlichen Einrichtungen.

Und: Derartige Sicherheitslücken werden auch nicht nur von Staatsschutz und Nachrichtendienst zur Terrorbekämpfung genutzt – sie sind ein Einfallstor für Kriminelle.

5. Mangelnder Rechtsschutz

Schließlich stellt sich – auch in Anbetracht der unzähligen Spyware-Skandale – die Frage: Wer überwacht die Überwacher und wie soll ein Missbrauch verhindert werden? Auch darauf liefert der vorliegende Gesetzesentwurf nur unzureichende Antworten und jedenfalls keinen ausreichenden Rechtsschutz.

In § 14 Abs 6 SNG wird geregelt, der Bundesminister für Inneres hat vor der erstmaligen Inbetriebnahme eines Programms zur Überwachung von Nachrichten und Informationen, die verschlüsselt gesendet, übermittelt oder empfangen werden, ‚*dem Rechtsschutzbeauftragten Gelegenheit zur Äußerung, ob das Programm den Anforderungen gemäß § 15b Abs. 1 entspricht, binnen zwei Wochen zu geben. Der tatsächliche Einsatz des Programms darf erst nach Ablauf dieser Frist oder Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten erfolgen.*‘

Der Rechtsschutzbeauftragte im Innenministerium ist ein Jurist. Dieser Jurist wird somit mit der technischen Beurteilung einer Software beauftragt, die enorm hohe Komplexität aufweist und deren Hersteller mit Sicherheit die volle Funktionsweise nicht offenlegen wird. Tatsächlich ist so eine Spyware im ständigen Schlagabtausch von Ausnutzung von Sicherheitslücken und deren Behebung unablässigen Änderungen unterworfen. Eine Vorab-Kontrolle könnte somit – selbst bei hinreichender technischer Versiertheit – immer nur für den Moment und keinesfalls als dauerhafte ‚Zertifizierung‘ gelten.

Äußert sich der Rechtsschutzbeauftragte nicht binnen 14 Tagen, so geht die Software auch ohne dessen Freigabe in Betrieb.

Doch nicht nur an dieser initialen Freigabe krankt der Rechtsschutz. Auch während einer laufenden Überwachung wird der Rechtsschutzbeauftragte die technischen Gegebenheiten des Zugriffs und das technische Missbrauchspotenzial kaum beurteilen können. Das Wesen derartiger Spyware-Produkte ist, dass sie ihre Funktionsweise ja gerade nicht offenlegen.

Schon im von ÖVP und FPÖ beschlossenen Bundestrojaner war dieser mangelhafte Rechtsschutz eines der Hauptargumente des VfGH für die Aufhebung. Der VfGH hat in seiner Bundestrojaner-Entscheidung ausgeführt: ‚*In Anbetracht der Intensität des Eingriffes in die Privatsphäre sämtlicher von einer Überwachung nach § 135a StPO betroffener Personen ist es unter dem Blickwinkel des Art 8 EMRK geboten, dass der Gesetzgeber eine begleitende, effektive – mit entsprechenden technischen Mitteln und personellen Ressourcen ausgestattete – und unabhängige Aufsicht über die laufende Durchführung der Maßnahme (durch einen Richter oder eine mit gleichwertigen Unabhängigkeitsgarantien ausgestattete Stelle) in jedem Fall sicherstellt.*‘

Wie schon beim Bundestrojaner 1 wird auch beim neuen Bundestrojaner der Rechtsschutz nicht hinreichend gewährleistet.

Somit gilt noch immer die Entscheidung des VfGH, dass eine solche Überwachung dem Grundrecht auf Privatsphäre widerspricht (VfGH 11.12.2019, G72/2019 ua)[15].

6. Verfassungswidrigkeit des Entwurfs

Der vorliegende Gesetzesentwurf ist somit aus mehreren Gründen verfassungswidrig:

- Der Entwurf baut darauf auf, dass der Staat bestehende Sicherheitslücken aktiv nutzt. Damit steht ein staatliches Interesse am Bestehen von Sicherheits-Schwachstellen in Computersystemen in diametralem Widerspruch zu einem staatlichen Auftrag, Netz- und Informationssystemsicherheit, aber auch die Privatsphäre seiner Bürger:innen zu schützen. Diese Verletzung positiver Schutzpflichten nach Art 8 EMRK, aber auch Art 10a StGG führt zur Verfassungswidrigkeit.
- Die behaupteten Beschränkungen der Überwachung nur auf Messenger-Kommunikation während des Überwachungszeitraums sind technisch nicht umsetzbar. Zudem ist die Installation der Spionage-Software nicht reversibel verwirklichbar.[16]
- Der Rechtsschutz ist nicht hinreichend gewährleistet – das betrifft sowohl die einmalige, nicht zwingende Vorab-Freigabe einer Spionage-Software als auch den Rechtsschutz, insbesondere vor und während der Überwachung.

7. Fazit

Der neue Gesetzesentwurf entspricht über weite Teile dem ihm zugrunde liegenden Ministerialentwurf 350/ME XXVII.GP, der bereits in Begutachtung war. Die Stellungnahmen zu diesem Entwurf waren vernichtend:

Technisch unausgereift bis technisch unmöglich, ein enormes Sicherheitsrisiko für unbescholtene Bürger:innen, Unternehmen und staatliche Institutionen, verfassungswidrig. Verwiesen wird auf die zahlreichen Stellungnahmen, von Universitäten, aber auch vom Rechtsanwaltskammertag, ÖGB, Bürgerrechtsorganisationen und der Vereinigung österreichischer Richterinnen und Richter, die die Ansicht der Grünen, dass hier massive Bedenken und klare Sicherheitsrisken bestehen, bestätigen.[17]

---

15 VfGH 11.12.2019, G72/2019 ua,
https://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20191211_19G00072_00/JFT_20191211_19G00072_00.pdf

16 Siehe die Stellungnahme des Fakultätsrats der TU Wien, https://informatics.tuwien.ac.at/news/1223;
siehe Stellungnahme von epicenter zum aktuellen Entwurf,
https://www.parlament.gv.at/PtWeb/api/s3serv/file/d99abd38-99eb-4ceb-a6b3-d44e41261afc

17 Stellungnahme des Instituts für Österreichisches und Europäisches Wirtschaftsstrafrecht der WU Wien,
https://www.parlament.gv.at/PtWeb/api/s3serv/file/58361fe5-e400-4a05-af97-f9de114a9767,
Stellungnahme von epicenter.works, https://www.parlament.gv.at/PtWeb/api/s3serv/file/308369fb-dbe7-42da-beaf-e900c8c40935, Stellungnahme von Univ.-Prof. Dr. René Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit, Univ.-Prof. Dr. Alois Birklbauer, Vorstand des Instituts für Strafrechtswissenschaften, Assoc.-Prof. Dr. Michael Sonntag, Stellvertretender Vorstand des Instituts für Netzwerke und Sicherheit an der Johannes Kepler Universität Linz,
https://www.parlament.gv.at/PtWeb/api/s3serv/file/4addf554-1f1b-4a9e-bd54-070f1749e5e5,
Stellungnahme des Österreichischen Rechtsanwaltskammertags,
https://www.parlament.gv.at/PtWeb/api/s3serv/file/7d9668bc-b53a-4064-9632-07bf9f76f1e3,

Diese Stellungnahmen – insbesondere jene, die die technischen Risken und Schwachstellen thematisieren – betreffen den neuen Gesetzesentwurf genauso wie den vorherigen.“

Der Ausschuss für innere Angelegenheiten hat den gegenständlichen Entschließungsantrag in seiner Sitzung am 2. Juli 2025 in Verhandlung genommen. An der Debatte beteiligten sich außer dem Berichterstatter Abgeordneten Süleyman **Zorba** die Abgeordneten Mag. Gernot **Darmann**, MMag. Dr. Michael **Schilchegger**, Douglas **Hoyos-Trauttmansdorff**, Maximilian **Köllner**, MA, Mag. Agnes Sirkka **Prammer**, Melanie **Erasim**, MSc und Mag. Friedrich **Ofenauer** sowie der Bundesminister für Inneres Mag. Gerhard **Karner**, der Staatssekretär im Bundesministerium für Inneres Mag. Jörg **Leichtfried** und der Ausschussobmann Abgeordnete Mag. Ernst **Gödl**.

Bei der Abstimmung fand der gegenständliche Entschließungsantrag der Abgeordneten Süleyman **Zorba**, Kolleginnen und Kollegen nicht die Zustimmung der Ausschussmehrheit (**für den Antrag:** F, G, **dagegen:** V, S, N).

Zum Berichterstatter für den Nationalrat wurde Abgeordneter Mag. Wolfgang **Gerstl** gewählt.

Als Ergebnis seiner Beratungen stellt der Ausschuss für innere Angelegenheiten somit den **Antrag**, der Nationalrat wolle diesen Bericht zur Kenntnis nehmen.

Wien, 2025 07 02

Mag. Wolfgang Gerstl	**Mag. Ernst Gödl**
Berichterstattung	Obmann

Stellungnahme des Österreichischen Gewerkschaftsbundes, https://www.parlament.gv.at/PtWeb/api/s3serv/file/2b6c0111-a26a-4d10-8f47-a2670e5aed9a, Stellungnahme der Vereinigung der österreichischen Richterinnen und Richter, https://www.parlament.gv.at/PtWeb/api/s3serv/file/6b78bb6d-aa6c-4a57-8f8d-a670923e6053 sowie zahlreiche weitere Stellungnahmen.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-09-05T18:19:51+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	