**248/A(E) XXVIII. GP**

**Eingebracht am 25.04.2025**


# ENTSCHLIESSUNGSANTRAG

der Abgeordneten Agnes-Sirkka Prammer, Süleyman Zorba, Freundinnen und Freunde

betreffend Bekenntnis zur echten Terrorbekämpfung statt Lizenz zur Massenüberwachung

## *BEGRÜNDUNG*

Nach einer Reihe von islamistischen Terroranschlägen in Europa wurde Österreich 2020 erstmals selbst Opfer eines solchen Angriffs. Im Jahr 2025 kam es zu einem weiteren Vorfall. Diese Ereignisse zeigen schmerzhaft, dass Terrorismusbekämpfung in Österreich höchste Priorität haben muss – um die Sicherheit aller Menschen zu gewährleisten, Radikalisierung frühzeitig zu verhindern und unsere demokratischen Werte zu schützen. Seit ihrer Neustrukturierung 2021 arbeitet die Direktion für Staatsschutz und Nachrichtendienst (DSN) mit hoher Professionalität genau an diesen Zielen.

Am 8. April 2025 wurde von Innenminister Karner ein neuer Entwurf für eine „Gefährder-Überwachung“ in Begutachtung geschickt – und damit einer langjährigen Forderung der ÖVP nachgekommen. Während das Vorhaben als notwendiger Schritt zur Terrorbekämpfung verkauft wird, zeigt eine genaue Durchsicht, dass es sich um die erneute Einführung eines Bundestrojaners handelt – einer Maßnahme, die bereits 2019 als verfassungswidrig aufgehoben wurde. Dabei wird in Handy- und Computersysteme eingedrungen, um auf sämtliche darauf gespeicherte Daten zuzugreifen. Geöffnet wird damit nicht nur der Zugang zu Messengerdiensten wie WhatsApp und ähnlichen Anbietern, sondern auch zu allen weiteren Daten auf den jeweiligen Geräten.

Wie mittlerweile mehrfach festgehalten, sind Computersysteme und insbesondere Handys wesentlicher Bestandteil der nach Art. 8 der Europäischen Menschenrechtskonvention geschützten Privatsphäre von Bürgerinnen und Bürgern. Unser gesamtes Leben ist auf diesen Geräten abgebildet - sie lassen Rückschlüsse auf persönliche Vorlieben, Neigungen, Orientierungen, Gesinnung und Lebensführung zu. Und diese Rückschlüsse betreffen nicht nur die überwachte Person selbst, sondern auch alle, die

auf deren Fotos erscheinen oder mit ihr in Kontakt stehen. Die Maßnahme ist somit deutlich tiefgreifender als alle Überwachungsinstrumente der Strafprozessordnung.

Hinzu kommt ein hohes Risiko des Missbrauchs. Erfahrungen aus anderen demokratischen Staaten Europas zeigen deutlich: Wird die Verwendung von Spyware freigegeben, ist ihr rechtswidriger Einsatz praktisch kaum zu verhindern. In den vergangenen Jahren wurden zahlreiche Skandale aufgedeckt, bei denen genau solche Systeme gegen Rechtsanwält:innen, Journalist:innen und zivilgesellschaftliche Akteur:innen eingesetzt wurden. Die Spuren führten zu Regierungen und Unternehmen in Polen, Ungarn, Griechenland, Zypern, Spanien, den Niederlanden, Belgien, Deutschland, Malta, Frankreich, Irland, Luxemburg, Italien – und auch nach Österreich.

Das stärkste Argument gegen die Einführung eines Bundestrojaners ist jedoch: Der österreichische Verfassungsschutz stößt bereits jetzt regelmäßig an seine Grenzen – nicht wegen fehlender gesetzlicher Befugnisse, sondern aufgrund zu geringer finanzieller und personeller Mittel, unzureichender Weiterbildungsmöglichkeiten für das Personal und veralteter technischer Ausstattung.

All dies führt dazu, dass der bestehende gesetzliche Rahmen nicht ausgeschöpft werden kann. Die Maßnahme des Bundestrojaners erscheint in diesem Zusammenhang als Scheinlösung – bestenfalls lenkt sie von den eigentlichen Problemen ab, schlimmstenfalls erweckt sie den Anschein, diese beheben zu können. Und das auf Kosten der Grundrechte und der Privatsphäre der Bürgerinnen und Bürger.

Dabei sollte der Bundesregierung und insbesondere dem Innenminister klar sein: Grundrechtsschutz ist keine Hürde für Sicherheit – er ist die Voraussetzung für nachhaltige Sicherheit.

Maßnahmen, die unterhalb der Schwelle eines Bundestrojaners liegen, bleibt der Innenminister bislang schuldig. Rechtsstaatliche Lösungen wie Open-Source-Forensik, bessere Hinweisgebersysteme oder strafrechtlich nachvollziehbare Informationsverwertung sind nicht nur grundrechtskonform, sondern auch praktikabel und wirksam. Moderne, auf Open-Source basierende forensische Tools ermöglichen eine transparente und gerichtsfeste Analyse digitaler Spuren – ohne verdeckten Zugriff auf Endgeräte. Verschlüsselte, anonyme Hinweisgebersysteme im Zusammenhang mit breit angelegten Präventions- und Sensibilisierungsmaßnahmen könnten dazu beitragen, extremistisches Gefahrenpotenzial frühzeitig zu erkennen – ohne massenhaft in private Kommunikation einzugreifen.

Und durch eine klare rechtliche Kette bei der Informationsverwertung – etwa durch Behördenzeugnisse, die es ermöglichen, geheime Erkenntnisse dennoch gerichtsverwertbar zu präsentieren – kann sichergestellt werden, dass Ermittlungen rechtlich tragfähig und demokratisch legitimiert bleiben. All diese Optionen liegen auf dem Tisch – doch der politische Wille, sie konsequent zu nutzen und weiterzuentwickeln, fehlt bislang.

Die unterfertigenden Abgeordneten stellen daher folgenden

## *ENTSCHLIESSUNGSANTRAG*

*Der Nationalrat wolle beschließen:*

„Die österreichische Bundesregierung, insbesondere der Bundesminister für Inneres, wird aufgefordert, ein wirksames Maßnahmenpaket zur Terrorismusbekämpfung vorzulegen, das die Direktion für Staatsschutz und Nachrichtendienst (DSN) strukturell stärkt – personell, finanziell und technisch – und dabei die Grundrechte aller in Österreich lebenden Menschen uneingeschränkt wahrt.

Das Maßnahmenpaket hat insbesondere folgende Punkte zu enthalten:

- Ein klares Bekenntnis der Regierung, auf jegliche finanziellen Kürzungen bei der DSN zu verzichten. Fort- und Weiterbildungsmaßnahmen müssen sofort wieder ermöglicht werden. Softwarelösungen zur Unterstützung bestehender Ermittlungsmethoden sind laufend zu evaluieren und technisch auf den neuesten Stand zu bringen.

- Ein klares Bekenntnis zu einer modernen und demokratisch legitimierten Sicherheitspolitik für die es zudem eine effektive Spionageabwehr – insbesondere durch Schutzmechanismen gegen den Einsatz gefährlicher Spionagesoftware durch feindliche Akteure braucht.

- Einführung eines sogenannten Behördenzeugnisses, das es der DSN ermöglicht, relevante Informationen mit der Strafverfolgung zu teilen, ohne Quellen oder geheimhaltungswürdige Details offenlegen zu müssen, um geheimdienstlich gewonnene Erkenntnisse auch rechtsstaatlich verwertbar zu machen. Die Beschuldigtenrechte und ein angemessenes Rechtsschutzniveau sind dabei zu wahren.

Die Einführung eines Bundestrojaners ist auszuschließen.“

*In formeller Hinsicht wird die Zuweisung an den Ausschuss für innere Angelegenheiten vorgeschlagen.*