321/AB
vom 20.02.2025 zu 327/J (XXVIII. GP)

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.041.217

Wien, am 20. Februar 2025

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat David Stögmüller, Freundinnen und Freunde haben am 20. Dezember 2024 unter der Nr. **327/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Beschaffung von Spionagesoftware“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1 bis 3 und 5 bis 7:

- *Ich ersuche um Übermittlung aller Dokumente des damaligen Vergabeverfahrens an den Unterausschuss des Ausschusses für Innere Angelegenheiten des Nationalrats.*
- *Wie erfolgte das öffentliche europäische Auswahlverfahren zur Anschaffung einer Spionagesoftware nach in Kraft treten des Gesetzes 2018?*
  - *a. Wann wurde es eingeleitet?*
  - *b. Wann wurde es eingestellt?*
  - *c. Welche gesonderten Richtlinien gibt es in der Zusammenarbeit mit Unternehmen für diesen besonders grundrechtsrelevanten aber auch sicherheitskritischen Bereich?*
    - *i. Wenn es keine gesonderten Richtlinien gibt, warum nicht und welche anderen Richtlinien werden in diesen Prozessen angewendet?*
    - *ii. Wenn es keine gesonderten Richtlinien gibt, werden diese für zukünftige Anschaffungen ausgearbeitet?*

d. *Mit welchen Anbietern wurden im Zuge dieses Verfahrens Gespräche geführt und welche Dokumente oder Informationen wurden von diesen übermittelt?*
e. *Wo genau wurde dieses Auswahlverfahren veröffentlicht?*
f. *Wie wurden die Anbieter ermittelt und ausgewählt?*
    i. *Von welchen europäischen Organisationseinheiten wurden Erfahrungswerte eingeholt? Welche Erfahrungswerte wurden hier geteilt?*
g. *Welche Anbieter wurden zur Legung von Angeboten eingeladen?*
h. *Welchen Sicherheitskriterien und/oder Richtlinien unterlagen die eingeladenen Anbieter?*
    i. *Wie wurde deren Hintergrund geprüft?*
    ii. *Wie sieht eine Eignungsprüfung für Unternehmen/Anbieter für eine solche Beschaffung genau aus?*
    iii. *Werden Verbindungen zu Russland, China oder den Iran aktiv überprüft?*
i. *Wie viele Angebote aus der Ausschreibung liegen dem Bundesministerium f. Inneres vor?*
j. *Wurde eine bestimmte Software angestrebt, die bereits von anderen Ministerien geprüft wurde?*
    i. *Wurde der Einsatz der Software der Firma DSIRF, die durch das Bundesministerium für Landesverteidigung getestet wurde, geprüft?*
k. *Wie hoch waren die Kosten der einzelnen Angebote für die Beschaffung der Software?*
l. *Wurde im Beschaffungsverfahren die Offenlegung des Quellcodes gefordert, um die Anwendung in der Strafverfolgung nachvollziehbar zu machen?*
    i. *Wenn nein, warum nicht?*
    ii. *Wird eine solche Offenlegung in Zukunft gefordert werden? Wenn nein, warum nicht?*

- *Mit den Erfahrungswerten des Beschaffungsvorgangs 2018, welche Kosten erwarten sie für eine Anschaffung einer zukünftigen Software auf Basis des am 14.8.2024 in Begutachtung geschickten Ministerialentwurfs (350/ME) zur Änderung des Staatsschutz- und Nachrichtendienstgesetzes?*
- *Laut dem Entwurf soll eine Überwachung auf laufende Messenger-Kommunikation beschränkt werden und keinen Komplett-Zugriff ermöglichen. Gem § 15 a Abs 5 ist technisch sicherzustellen, dass 1. ausschließlich innerhalb des Bewilligungszeitraums 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. Ausdrücklich wird in den Erläuterungen festgehalten: „Die*

einzubringende Software ist technisch regulierbar, sodass nur gezielte und von der Bewilligung umfasste Nachrichten aus bestimmten Applikationen ausgeleitet werden können". In der Begutachtung wurde in mehreren Stellungnahmen ausgeführt, dass eine derartige technische Spezifikation nicht möglich ist.

   i. *Gibt es konkrete Angebote, die diese technischen Spezifikationen erfüllen?*
   ii. *Wenn ja, wer hat diese Angebote gestellt?*
   iii. *Wie sollen die in den Erläuterungen dargestellten Beschränkungen sichergestellt werden?*
   iv. *Gibt es dazu konkrete Machbarkeits-Analysen?*
   v. *Wenn ja, wer hat diese Analysen durchgeführt?*

- *Wie soll sichergestellt werden, dass Sicherheitslücken in Endgeräten, die für die Einbringung der Überwachungssoftware genutzt werden sollen, nicht von Geheimdiensten und ausländischen Regierungen oder kriminellen Organisationen genutzt werden können? Gibt es ein Software-Angebot, das hier eine technisch nachvollziehbare Lösung beinhaltet?*
   i. *Wenn ja, wer hat dieses Angebot gestellt?*
- *Wie soll die gesetzlich vorgesehene Spezifikation für die Überwachungssoftware überprüft werden. Ist eine Zertifizierung durch eine unabhängige Stelle vorgesehen?*
   i. *Welche Zertifizierungsstelle soll das sein?*

Das anfragengegenständlich Vergabeverfahren wurde im Dezember 2018 eingeleitet, nach den Grundsätzen des Bundesvergabegesetzes Verteidigung Sicherheit 2012 (BVergGVS 2012) geführt und im Dezember 2019 aufgrund des Erkenntnisses des Verfassungsgerichtshofes eingestellt. Die im Beschaffungsvorgang verarbeiteten Informationen zu den diesbezüglichen, besonders sensiblen Ermittlungsmaßnahmen zur Bekämpfung von Terrorismus und organisierter Schwerkriminalität waren entsprechend den Erfordernissen klassifiziert und dürfen daher nicht im Rahmen der Beantwortung der gegenständlichen Anfrage erörtert werden. Die Beschaffung der für die Überwachung von verschlüsselten Nachrichten benötigten Hard- und Software für die Zwecke der effektiven Bekämpfung verfassungsschutzrelevanter Bedrohungslagen im Sinne des Ministerialentwurfs 350/ME XXVII. GP erfordert gleichfalls den Umgang mit klassifizierten Informationen und die strikte Wahrung von Vertraulichkeit.

Von einer detaillierten Beantwortung der Fragen muss Abstand genommen werden, da aus jedweder Beantwortung zu technischen Spezifikationen der Software oder zum Anbieter Rückschlüsse gezogen werden können, welche die Abwehrfähigkeit der vom Verfassungsschutz beobachteten Personen erhöhen und künftige Ermittlungsmaßnahmen

in den Bereichen des internationalen Terrorismus oder der Spionageabwehr wesentlich erschweren.

Zur ausführlicheren Beantwortung darf auf den Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten gemäß Artikel 52 Bundes-Verfassungsgesetz hingewiesen werden, indem die parlamentarische Kontrolle unter Wahrung der – für die Aufgabenerfüllung der Staatsschutzbehörden notwendigen – Vertraulichkeit ausgeübt wird.

Zur Frage 4:

- *Mit den Erfahrungswerten rund um die Überwachung von Journalist:innen, Anwält:innen und Oppositionellen durch die Spioange-Software Pegasus, werden sie besondere Vorkehrungen in einer zukünftigen Software verlangen, damit keine Überwachung der obengenannten Personengruppen möglich ist?*

Die Überwachung von Nachrichten, die verschlüsselt gesendet, übermittelt oder empfangen werden, ist nur zur Vorbeugung gesetzlich determinierter, besonders schwerwiegender verfassungsgefährdender Angriffe durch eine Person erlaubt. Unter derartigen Angriffen sind ausschließlich verfassungsgefährdende Angriffe zu verstehen, die im Falle ihrer Verwirklichung zumindest mit bis zu zehn Jahren Freiheitsstrafe bedroht sind oder den Tatbestand des § 256 Strafgesetzbuch erfüllen. Die Ermittlungsmaßnahme trägt dem ultima ratio-Prinzip Rechnung und bleibt auf Einzelfälle beschränkt. Zudem ist gemäß § 9 Staatsschutz- und Nachrichtendienst-Gesetz bereits gegenwärtig bei Ermittlungen von personenbezogenen Daten ein Eingriff in das von § 157 Abs. 1 Z 2 bis 4 Strafprozessordnung geschützte Recht nicht zulässig.

Gerhard Karner

	Datum/Zeit	2025-02-20T15:13:27+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	148769640
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-02-20T15:19:03+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	