

 **Bundesministerium
Inneres**

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2021-0.580.421

Wien, am 22. September 2021

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Dr. Nikolaus Scherak, MA, Kolleginnen und Kollegen haben am 23. Juli 2021 unter der Nr. **7556/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Überwachung von Österreicher_innen durch Spionageprogramme wie Pegasus“ gerichtet.

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

Zur Frage 1:

- *Wusste Ihr Ministerium vor Veröffentlichung der über 50.000 Telefonnummern auf der Pegasus-Überwachungsliste davon, dass auch ein Österreicher auf dieser Liste steht?*
 - a. *Wenn ja, warum wurde nichts dagegen unternommen?*

Nein.

Zu den Fragen 2 bis 4 und 12:

- *Welche Maßnahmen wurden von Ihrem Ministerium bisher getroffen, um eine Überwachung österreichischer Bürger_innen durch ausländische Spionageprogramme zu vermeiden?*

- *Nach Bekanntwerden der Überwachung eines Österreichers durch das Spionageprogramm Pegasus: Wie wollen Sie die Überwachung von Bürger_innen durch ausländische Spionageprogramme zukünftig verhindern?*
- *Nach Bekanntwerden der Überwachung eines Österreichers durch das Spionageprogramm Pegasus: Sind weitere Maßnahmen zum Schutz der Privatsphäre von Österreichern und Österreichern in Zusammenhang mit Überwachungsprogrammen in Planung?*
 - a. *Wenn nein, weshalb nicht?*
- *In Beantwortung 4352/AB unserer Anfrage 4314/J führte das BMI aus, dass sich Österreich für einen rechtmäßigen Zugriff für Strafverfolgungsbehörden auf verschlüsselte Kommunikation eingesetzt hat. Ein solcher Zugriff erfolge laut BMI nur im Einklang mit den Grundrechten und im Rahmen der gesetzlichen Bestimmungen. Konkret wurde jedoch offen gelassen wie ein verfassungskonformer, unter Wahrung der Privatsphäre und der Grundrechte gestalteter Zugriff der Strafverfolgungsbehörden auf verschlüsselte Kommunikation im Detail aussehen könnte. Wurde mittlerweile eine Rechtsgrundlage für den Zugriff der Strafverfolgungsbehörden auf verschlüsselte Kommunikation geschaffen?*

Die Infizierung von Endgeräten der Bürgerinnen und Bürger Österreichs mit ausländischen Spionageprogrammen könnte in technischer Hinsicht nur durch gleichzeitige, umfassende technische Überwachung sämtlicher Geräte durch die Sicherheitsbehörden verhindert werden, wobei selbst mit einer derart eingriffsintensiven Maßnahme kein hundertprozentiger Schutz verbunden wäre. Dass ein derartiges Vorgehen im klaren Widerspruch zur Wahrung der Privatsphäre und den Grundrechten der österreichischen Bevölkerung stünde und somit keine Deckung in der österreichischen Rechtsordnung fände, bedarf keiner weiteren Ausführungen.

Wie ich in meiner Beantwortung der zitierten Anfrage 4314/J XXVII. GP (4352/AB XXVII. GP) erläutert habe, muss jeder Zugriff der Strafverfolgungsbehörden auf verschlüsselte Kommunikation im Einklang mit der österreichischen Verfassung und im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs erfolgen. Die diesbezügliche Ausgestaltung eines solchen Zugriffs ist weiterhin offen.

Zu den Fragen 5 und 6 sowie 9 und 10:

- *Nach Bekanntwerden des Einsatzes von Pegasus in Ungarn und somit innerhalb der EU: Welche Position bezieht Ihr Ministerium im Umgang mit dem Einsatz von Spionagesoftwares durch andere Staaten und im Speziellen durch EU-Mitgliedsstaaten?*

- Sind Sie mit Ihren Amtskolleg_innen aus anderen EU-Mitgliedsstaaten in Bezug auf den Einsatz von und den Umgang mit Spionageprogrammen wie Pegasus im Austausch?
 - a. Wenn ja, welche Position vertreten Sie dort?
 - b. Wenn ja, was ist der aktuelle Stand des Austauschs?
 - c. Wenn nein, ist ein solcher Austausch in Planung?
- Die Bundesregierung strebt eine "strategische Partnerschaft" mit den Vereinigten Arabischen Emiraten (VAE) an. Steht/stand Ihr Ministerium in Bezug auf Spionageprogramme wie Pegasus im Austausch mit den VAE?
 - a. Wenn ja, welcher Zweck wird mit diesem Austausch verfolgt?
 - b. Wenn ja, was ist der aktuelle Stand des Austauschs?
 - c. Wenn nein, ist ein diesbezüglicher Austausch in Planung?
- Steht/stand Ihr Ministerium in Bezug auf Spionageprogramme wie Pegasus im Austausch mit Ungarn?
 - a. Wenn ja, welcher Zweck wird mit diesem Austausch verfolgt?
 - b. Wenn ja, was ist der aktuelle Stand des Austauschs?
 - c. Wenn nein, ist ein diesbezüglicher Austausch in Planung?

Es findet im Bereich meines Ressorts auf internationaler Ebene kein Informationsaustausch im Zusammenhang mit der Verwendung von Spionageprogrammen statt.

Zu den Fragen 7 und 8:

- Ist/war Ihr Ministerium Kunde des israelischen Unternehmens NSO Group?
 - a. Wenn ja, welche/s Produkt/e der NSO Group wird/werden bezogen?
 - b. Wenn nein, ist eine Zusammenarbeit mit der NSO Group in Planung?
- Steht/stand Ihr Ministerium im Austausch mit dem israelischen Unternehmen NSO Group?
 - a. Wenn ja, welcher Zweck wird mit diesem Austausch verfolgt?
 - b. Wenn ja, was ist der aktuelle Stand des Austauschs?
 - c. Wenn nein, ist ein Austausch mit der NSO Group in Planung?

Nein.

Zur Frage 11:

- Ohne Sicherheitslücken bewusst offen zu halten, ist die Umsetzung eines funktionierenden Bundestrojaners nicht möglich. Der Pegasus-Skandal zeigt deutlich, wie gefährlich diese Sicherheitslücken für Bürger_innen sein können und wie anfällig diese Sicherheitslücken Bürger_innen für ausländische Spionageangriffe machen. Sollte

vor diesem Hintergrund nicht von der Schaffung und Nutzung eines Bundestrojaners abgesehen werden?

Dem Fragerrecht gemäß Art. 52 B-VG und § 90 des Geschäftsordnungsgesetzes 1975 unterliegen nur Handlungen und Unterlassungen. Kein Gegenstand des Interpellationsrechts sind daher bloße Meinungen und Einschätzungen.

Karl Nehammer, MSc

