

## **Kleine Anfrage**

**der Abgeordneten Jan Korte, Sevim Dağdelen, Anke Domscheit-Berg, Andrej Hunko, Ulla Jelpke, Žaklin Nastić, Thomas Nord, Petra Pau, Tobias Pflüger, Eva-Maria Schreiber, Dr. Kirsten Tackmann, Kathrin Vogler und der Fraktion DIE LINKE.**

### **Einsatz der Spionagesoftware „Pegasus“ in Deutschland**

Nach Berichten eines internationalen Rechercheverbundes zahlreicher Medien, an dem aus Deutschland die „Süddeutsche Zeitung“, der „NDR“, „WDR“ und die Wochenzeitung „ZEIT“ beteiligt sind, sollen Regierungen weltweit „militärische Spionagesoftware“ der israelischen Firma NSO Group nicht nur für die Überwachung von Terroristen und Kriminellen nutzen, sondern auch für erfolgreiche Hacks von Smartphones, die Journalisten, Menschenrechtsaktivisten und Geschäftsleuten gehörten. Mit der Software, die als eine der leistungsfähigsten Spionageprogramme auf dem kommerziellen Markt gilt, kann „unbemerkt die komplette Kommunikation auf dem Mobiltelefon einer Zielperson überwacht werden kann – egal ob SMS, E-Mails oder verschlüsselte Chats. Auch Fotos und Videos können durchsucht und Passwörter ausgelesen werden. Und das alles sogar aus der Ferne, ohne physischen Zugriff auf das Telefon zu haben.“ (<https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html>). Die Smartphones können aber nicht nur heimlich überwacht und komplett ausgespäht werden, sondern sogar zu Wanzen umgewandelt werden, um unbemerkt Gespräche mitzuschneiden, wobei neben dem Mikrofon auch die Kamera eines Geräts unbemerkt eingeschaltet werden könne. Während auf der NSO-Website die Firma ihre Produkte als „Technologie, die Regierungsbehörden hilft, Terrorismus und Verbrechen zu verhindern und zu untersuchen“ anpreist, zeigen die Medienrecherchen, die sich auch auf Daten von Amnesty International stützen, dass mindestens 189 Journalistinnen und Journalisten, 85 Menschenrechtsaktivistinnen und Menschenrechtsaktivisten und mehr als 600 Politikerinnen und Politiker mit der Spionagesoftware weltweit ausgespäht wurden. Amnesty International hatte gemeinsam mit der Organisation Forbidden Stories einen Datensatz von mehr als 50 000 Telefonnummern ausgewertet, die als potenzielle Ausspähziele von Kunden der NSO Group ausgewählt worden seien. Unter den Ausgespähten finden sich auch investigative Journalisten aus Ungarn, Marokko oder Aserbaidschan sowie beispielsweise katalonische Unabhängigkeitsbefürworter in Spanien. Am 20. Juli 2021 berichtete u. a. „Spiegel Online“, dass unter den zahlreichen Ausgespähten auch etliche europäische Spitzenpolitiker, wie etwa der französische Präsident Emmanuel Macron und sein direktes Umfeld, „der damalige Premierminister Édouard Philippe sowie mehrere Ministerinnen und Minister in Frankreich ausgespäht werden, unter ihnen die noch amtierenden Kabinettsmitglieder Außenminister Jean-Yves Le Drian, Wirtschaftsminister Bruno Le Maire und Bildungsminister Jean-Michel Blanquer“ seien (<https://www.spiegel.de/ausland/pegasus-emmanu>

el-macron-im-visier-der-cyberwaffe-a-28bfa163-4933-41af-8128-9d63ed5e2501). Besonders exzessiv ist die Software offenbar in Mexiko zum Einsatz gekommen, wo neben Journalisten u. a. auch das Umfeld des amtierenden Präsidenten ausgeforscht wurde (vgl. <https://www.tagesschau.de/investigativ/ndr-wdr/spionage-software-pegasus-mexiko-101.html>). Laut forensischem Bericht von Amnesty International (<https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>) zählten zur „Pegasus“-Infrastruktur auch 212 DNS-Server in Deutschland. Am 20. Juli 2021 berichtete RND, dass das Büro der Pariser Staatsanwaltschaft Ermittlungen zum mutmaßlich weit verbreiteten Einsatz der Spionagesoftware gegen Journalisten, Menschenrechtsaktivisten und Dissidenten in Frankreich aufgenommen habe und zu einer ganzen Reihe möglicher Anklagepunkte, darunter Verstoß gegen das Persönlichkeitsrecht, illegale Nutzung von Daten und illegaler Verkauf von Spionagesoftware, ermittelt werde.

In Deutschland ist die am 6. April 2017 errichtete Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat damit betraut, Bundesbehörden mit Sicherheitsaufgaben im Hinblick auf informationstechnische Fähigkeiten zu unterstützen und zu beraten. Die ZITiS-IT-Fachleute entwickeln u. a. selbst Cyberwerkzeuge, mit denen Polizei und Verfassungsschutz verschlüsselte Kommunikation überwachen können, sichten aber auch den weltweiten Markt an Überwachungssoftware, deren Kauf sich für deutsche Sicherheitsbehörden lohnen könnte. Laut Bericht der „Tagesschau“ sollen NSO-Vertreter bei ZITiS 2018 in München vorstellig geworden sein: „Sie waren auf einer Art Roadshow und präsentierten ihr Portfolio“ (<https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html>), in dem sich auch die Spionagesoftware Pegasus befunden habe. „Ein Jahr zuvor, im Oktober 2017, wurde NSO schon beim Bundeskriminalamt (BKA) in Wiesbaden vorstellig. Ebenso gab es Gespräche mit dem BND und dem Bundesamt für Verfassungsschutz. Mit den Cyberexperten vom bayerischen Landeskriminalamt (LKA) trafen sich die Vertreter der israelischen Firma im Jahr 2019 sogar gleich zwei Mal. Bei einer weiteren Vorführung im September 2019 im Innenministerium in München war sogar Minister Joachim Herrmann anwesend, wie ein Sprecher mitteilte“ (ebd.). Bislang habe NSO in Deutschland aber „wohl nur Absagen“ erhalten, während es „an 60 unterschiedliche Behörden in 40 Ländern der Welt [...] seine Produkte nach eigenen Angaben bereits verkauft“ hat (ebd.).

Am 21. Juli 2021 stellte das Bundesverfassungsgericht in seinem veröffentlichten Beschluss (1 BvR 2771/18; „IT-Sicherheitslücken“) klar, dass sich aus Artikel 10 des Grundgesetzes (GG) eine Schutzpflicht bezüglich bekannter Sicherheitslücken ergibt und „die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet den Staat, zum Schutz der Systeme vor Angriffen durch Dritte beizutragen“ ([https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608\\_1bvr277118.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608_1bvr277118.html)).

Wir fragen die Bundesregierung:

1. Kann die Bundesregierung die Medienberichte über Treffen, Produktpräsentationen und Verkaufsgespräche zwischen NSO-Vertretern und Vertretern deutscher Sicherheitsbehörden bestätigen, und wenn ja, wann fanden diese jeweils statt (bitte entsprechend nach Datum, Behörde und Thema des Treffens auflisten)?

2. Haben nach Kenntnis der Bundesregierung deutsche Sicherheitsbehörden Produkte der Firma NSO Group erworben, und wenn ja, um welche Sicherheitsbehörden und Produkte handelt es sich dabei (bitte entsprechend nach Sicherheitsbehörde, Produkt, Kostenaufwand und Anzahl der Einsätze aufführen)?
3. Wurden deutschen Sicherheitsbehörden von der Firma NSO Group Produkte und/oder Leistungen für Testzwecke (z. B. zeitlich terminierte Testversionen) übermittelt?  
Wenn ja, in welchem Umfang, und über welchen Zeitraum?  
Wurden besagte Testversionen dann auch ausgeführt?
4. Sofern die Spionagesoftware „Pegasus“ zwar von deutschen Behörden beschafft, aber bislang nicht eingesetzt wurde, worin bestanden bzw. bestehen die Gründe?
5. Hat die Bundesregierung einen Einsatz der Spionagesoftware „Pegasus“ in Deutschland in rechtlicher Hinsicht bewertet, und wenn ja, mit welchem Ergebnis?
6. Hat die Bundesregierung den Betrieb von Servern der Firma NSO Group in Deutschland zur weltweiten Anwendung der Spionagesoftware „Pegasus“ in rechtlicher Hinsicht bewertet, und sieht sie ggf. Handlungsbedarf (bitte begründen)?
7. Stellen nach Rechtsauffassung der Bundesregierung das Anbieten und der Verkauf der Spionagesoftware „Pegasus“ in Deutschland Straftatbestände nach dem Strafgesetzbuch (StGB) oder nach anderen Rechtsnormen dar, und wenn ja, welche (bitte begründen)?
8. Hat die Bundesregierung einen Einsatz der Spionagesoftware „Pegasus“ in Deutschland im Hinblick auf eine Gefährdung der grundrechtlich geschützten Meinungs-, Informations-, Presse-, Rundfunk- und Filmfreiheit (Artikel 5 Absatz 1 und 2 GG) bewertet, und wenn ja, mit welchem Ergebnis (bitte begründen)?
9. Haben die Bundesregierung und deutsche Sicherheitsbehörden Kenntnis über die Ausspähung in der Bundesrepublik Deutschland lebender Journalistinnen und Journalisten, Politikerinnen und Politikern oder Menschenrechtsaktivistinnen und Menschenrechtsaktivisten mithilfe der Spionagesoftware „Pegasus“, wenn ja,
  - a) durch wen erfolgt die Überwachung,
  - b) wer ist davon betroffen,
  - c) seit wann besitzt die Bundesregierung diese Informationen,
  - d) wurden die zuständigen parlamentarischen Kontrollgremien des Deutschen Bundestages davon in Kenntnis gesetzt, falls nein, weshalb nicht,
  - e) wurden Betroffene seitens deutscher Sicherheitsbehörden informiert, und wenn ja, wann, und wenn nein, warum nicht?

10. Hat die Bundesregierung überprüft, ob Angehörige der Bundesregierung selbst von Überwachungsmaßnahmen betroffen sind, weil diese in direktem Austausch bzw. Kontakt mit überwachten ausländischen Regierungsangehörigen standen (inklusive Staats- und Regierungschefs, beispielsweise Emmanuel Macron), und wenn ja, mit welchem Ergebnis, und gab es in diesem Zusammenhang Konsultationen mit anderen Regierungen?
11. Ist der Bundesregierung bekannt, ob unter Einsatz von Spionageprodukten der Firma NSO Group auch Rechner und Informationssysteme von an Asylverfahren beteiligten Einrichtungen, vor allem des Bundes, Ziel der Ausspähung durch Geheimdienste von Staaten sind, die Oppositionelle verfolgen?
  - a) Sind der Bundesregierung derartige Angriffe bekannt, und wenn ja, auf welche Einrichtungen sind diese wann, von wem und mit welchem Ziel jeweils erfolgt, und welche Konsequenzen seitens der Sicherheitsbehörden, des Bundesamts für Sicherheit in der Informationstechnik oder des Verfassungsschutzes hatte dies jeweils?

Wenn nein, haben die Bundesregierung und deutsche Sicherheitsbehörden eine mögliche Ausspähung untersucht, oder werden sie eine solche Untersuchung veranlassen?
  - b) Sind der Bundesregierung grundsätzlich Angriffe auf die Kommunikationsinfrastruktur des Bundes bzw. in Deutschland bekannt, die mit Produkten der Firma NSO Group verübt wurden?

Wenn ja, welche sind dies, und wie wurde darauf seitens der Sicherheitsbehörden reagiert?
12. Wie beabsichtigt die Bundesregierung, ihrer Schutzpflicht gegenüber ihren Bürgerinnen und Bürgern, aber auch gegenüber ausländischen Betroffenen (z. B. Journalisten, Menschenrechtsaktivisten und Asylsuchenden) in Deutschland nachzukommen und sie vor Zugriffen ausländischer Geheimdienste zu schützen?
13. Was hat die Bundesregierung bislang zum Schutz der Bevölkerung vor Ausspähung durch Spionagesoftware auf deutscher und europäischer Ebene unternommen, und wie ist der aktuelle Umsetzungsstand beim staatlichen Schwachstellenmanagement (Vulnerability Equities Process – VEP)?
14. Wie hoch waren seit 2017 die Kosten für die Entwicklung bzw. die Beschaffung und den Einsatz von Überwachungssoftware von Bundessicherheitsbehörden (bitte entsprechend nach Jahr, Behörde, Erwerb, Entwicklung und Einsatz von Überwachungssoftware aufschlüsseln)?
15. Wie hoch waren seit 2017 die Kosten für die Entwicklung bzw. die Beschaffung und den Einsatz von Verschlüsselungs- und Antivirensoftware durch Bundesbehörden (bitte entsprechend nach Jahr, Behörde, Beschaffung, Entwicklung und Einsatz von Verschlüsselungs- und Antivirensoftware aufschlüsseln)?
16. Kann die Bundesregierung ausschließen, dass die von Einrichtungen des Bundes entwickelten bzw. geheim gehaltenen Sicherheitslücken von der NSO Group Technologies für ihre Produkte und/oder Leistungen verwendet werden, um weltweit elektronische Geräte zu kompromittieren (bitte begründen)?

17. Kennt die Bundesregierung die Forderung des Whistleblower Edward Snowden nach einem Moratorium für den Handel mit Cyberwaffen (vgl. <https://www.zeit.de/digital/2021-07/edward-snowden-spionage-software-pegasus-handly-ueberwachung-diktaturen>), und hat sie eine Position dazu?

Wird sie diese Forderung umsetzen?

Wenn nein, warum nicht?

18. Kennt die Bundesregierung die Forderung des Deutschen Journalistenverbandes (DJV), die deutschen Sicherheitsbehörden und die Geheimdienste sollen Auskunft darüber geben, ob die „Pegasus“-Spähsoftware gegen deutsche Journalistinnen und Journalisten eingesetzt wurde (<https://www.djv.de/startseite/profil/der-djv/pressebereich-download/pressemitteilungen/detail/news-aufklaerung-gefordert-2>), und wird sie darauf reagieren?

Wenn ja, in welcher Form (bitte begründen)?

19. Wie hat oder wird die Bundesregierung auf die Forderung der Vereinten Nationen nach einer menschenrechtszentrierten Regulierung solcher Überwachungssoftware reagieren (<https://news.un.org/en/story/2021/07/1096142>; bitte begründen)?

Berlin, 25. Juli 2021

**Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion**





