

Bundeskriminalamt
IFG-Sachbearbeitung
Thaerstraße 11
65193 Wiesbaden

25. August 2022

IFG: Vertrag über NSO Pegasus [#253992] - Widerspruch

Sehr geehrte Damen und Herren,

Gegen Ihren Bescheid vom 10. August 2022 mit dem Zeichen IFG - 2022-0020798112 lege ich Widerspruch ein.

Sie argumentieren, dass der Erwerb des Produkts "Pegasus" des israelischen Unternehmens NSO Group nicht öffentlich bekannt werden darf. Dieser Fakt ist jedoch bereits öffentlich bekannt.

Bereits in meiner Anfrage habe ich die Berichterstattung der Tagesschau verlinkt, die vor einem Jahr schrieb: „BKA kaufte Spionagesoftware bei NSO“:

<https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-101.html>

Darüber hinaus gibt es weitere Berichterstattung. Die Tagesschau schreibt in einem weiteren Artikel: „Am Dienstagmorgen nun, wenn auch hinter verschlossener Tür, brachen das Bundesinnenministerium und das Bundeskriminalamt (BKA) ihr Schweigen. Ja, das BKA habe eine Version der ‚Pegasus‘-Software eingekauft, soll die Vize-Behördenchefin Martina Link den Parlamentariern im Innenausschuss bestätigt haben.“

<https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software->

netzpolitik.org e. V.
Schönhauser Allee 6/7
10119 Berlin

kontakt@netzpolitik.org
netzpolitik.org

Vereinsitz:
Berlin

Registernummer:
VR 32395 B

Registergericht:
AG Charlottenburg, Berlin

Vorsitzende:
Christina Köver

Steuernummer:
27/673/54182
Finanzamt für
Körperschaften I

USt-IdNr.:
DE 316038383

Bankverbindung:
netzpolitik.org e.V.
DE62 4306 0967 1149 2784
00
GENODEM1GLS

[pegasus-smartphone-103.html](https://www.legaltribune.de/pegasus-smartphone-103.html)

Die Legal Tribute Online schreibt: „Das BKA hat die umstrittene Spähsoftware ‚Pegasus‘ von der israelischen NSO Group erworben.“

<https://www.lto.de/recht/hintergruende/h/spysoftware-pegasus-bka-einsatz/>

Die Zeit schreibt sogar: „BKA hat NSO-Spähstrojaner bereits mehrfach eingesetzt“.

<https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel/komplettansicht>

Diese Informationen stehen auch auf Wikipedia. Im Artikel für „Pegasus (Spyware)“ haben Deutschland und das BKA einen eigenen Absatz, auf deutsch: [https://de.wikipedia.org/wiki/Pegasus_\(Spyware\)#Deutschland](https://de.wikipedia.org/wiki/Pegasus_(Spyware)#Deutschland) und auf englisch:

[https://en.wikipedia.org/wiki/Pegasus_\(spyware\)#Germany](https://en.wikipedia.org/wiki/Pegasus_(spyware)#Germany)

Auch offizielle Stellen verwenden und verbreiten diese Informationen.

Der Deutsche Bundestag hat im Plenum über den Einsatz von Pegasus diskutiert: <https://www.bundestag.de/dokumente/textarchiv/2022/kw07-de-spaehsoftware-881048>

Dort haben mehrere Mitglieder:innen des Bundestags zugegeben, dass das BKA Pegasus besitzt und einsetzt. So sagte etwa der Abgeordnete Uli Grötsch von der Regierungspartei SPD: „Das Bundeskriminalamt, das Sie eben angesprochen haben, setzt Pegasus – und das auch nur in ganz wenigen Bereichen – auf die gleiche Art und Weise ein.“

<https://dserver.bundestag.de/btp/20/20018.pdf#P.1319>

Die Frage, ob Bundesbehörden wie das BKA „in Kontakt mit der NSO Group steht oder nicht“, hat sogar die Bundesregierung ganz offiziell auf eine Kleine Anfrage im Bundestag beantwortet: „Zur Wahrnehmung ihrer Aufgaben hinsichtlich der Weiterentwicklung von Cyberfähigkeiten im Bereich der Informationstechnischen Überwachung steht die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) seit 2018 mit Vertretern der NSO Group Technologies Limited in Kontakt, um im Rahmen einer Marktsichtung Informationen über das Portfolio des Unternehmens zu erhalten und dessen Eignung für eine mögliche Verwendung durch die Sicherheitsbehörden des Bundes zu evaluieren.“

<https://dserver.bundestag.de/btd/19/322/1932246.pdf>

Das Europäische Parlament hat einen „Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware“ eingesetzt:

<https://www.europarl.europa.eu/committees/de/pega/home/highlights>

Der Wissenschaftliche Dienst des Europäischen Parlaments hat eine Studie zum Thema Pegasus erstellt, die enthält ebenfalls ein Kapitel zum Thema Pegasus in Deutschland und beim BKA:

[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EP_RS_STU\(2022\)729397_EN.pdf#page=32](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EP_RS_STU(2022)729397_EN.pdf#page=32)

Im Herbst wird der Untersuchungsausschuss das Thema Pegasus in Deutschland an einem dedizierten Termin behandeln.

Die Firma NSO Group hat bereits in diesem Untersuchungsausschuss ausgesagt: <https://netzpolitik.org/2022/untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/>

NSO hat gegenüber dem Untersuchungsausschuss einerseits gesagt, wie viele EU-Staaten Pegasus nutzen: „Es gibt 12 EU-Mitgliedsländer, die 15 Pegasus-Systeme nutzen (einige Länder haben mehr als ein System erworben). Insgesamt gibt es 22 Regierungsorganisationen in EU-Ländern, die das Pegasus-System nutzen (in einigen Ländern wurde das System für die Nutzung durch mehr als eine Organisation erworben, von denen jede das Endnutzungszertifikat unterzeichnet). Wir hatten Verträge für Pegasus mit 2 weiteren EU-Mitgliedsländern, die inzwischen gekündigt wurden.“ <https://netzpolitik.org/2022/nso-group-zwoelf-eu-laender-nutzen-pegasus-staatstrojaner/>

NSO hat gegenüber dem Untersuchungsausschuss andererseits gesagt, dass die „Regierungen der einzelnen EU-Mitgliedsländer“ Auskunft über Pegasus geben dürfen: „Es geht um ihre Sicherheit, und sie können entscheiden, ob sie diese Frage diskutieren wollen oder nicht.“

https://netzpolitik.org/2022/untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/#2022-06-21_European-Parliament_PEGA_NSO

Vor diesem Hintergrund ist es nicht nachvollziehbar, welche nachteiligen Auswirkungen das Bekanntwerden der Information auf internationale Beziehungen haben soll. § 3 Nr. 1 a) IFG greift nicht.

Die Information hat auch keine nachteiligen Auswirkungen auf Belange

der inneren oder äußeren Sicherheit oder gefährdet sogar die öffentliche Sicherheit. Dass das BKA die Software Pegasus besitzt und einsetzt, ist bereits bekannt. Dass das BKA die informationstechnischen Überwachungsmaßnahmen Quellen-TKÜ und Online-Durchsuchung einsetzen darf, steht im Gesetz:

https://www.gesetze-im-internet.de/stpo/_100a.html

https://www.gesetze-im-internet.de/stpo/_100b.html

Das BKA schreibt sogar selbst auf seiner Webseite: „Das BKA verfügt sowohl über eigenentwickelte als auch über kommerzielle Software zur Durchführung von Maßnahmen zur Quellen-TKÜ.“ Und „Das BKA verfügt über Software zur Durchführung von Maßnahmen der Online-Durchsuchung.“

https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Tecnologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html

Dass (und wie oft) das Ermittlungsbehörden wie das BKA diese Software einsetzen, geht aus aus den offiziellen Zahlen des Bundesamts für Justiz zur Telekommunikationsüberwachung hervor:

https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistik/Uebersicht_TKUE_2020.pdf?__blob=publicationFile

https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistik/Uebersicht_Online_Durchsuchung_2020.pdf?__blob=publicationFile

Die Information, dass das BKA die Maßnahmen Quellen-TKÜ und Online-Durchsuchung (auch) mit dem Produkt NSO Pegasus durchführt, gefährdet die Maßnahme nicht.

Das VG Wiesbaden hat mit Urteil zum Vertrag des Konkurrenz-Produkts FinFisher ausgeführt (6 K 687/15.WI): „Gleiches gilt auch für § 3 Nr. 2 IFG (Bekanntwerden der Informationen, das die öffentliche Sicherheit gefährden kann). Denn zu keinem der benannten Punkte hat das Bundeskriminalamt darlegen können, dass das Bekanntwerden der Informationen die öffentliche Sicherheit gefährden kann. Eine konkrete Gefährdung eines Schutzgutes und wenn ja, welches, hat das Bundeskriminalamt nicht dargelegt. Dass bei Bekanntwerden näherer Informationen über den ‚Bundestrojaner‘ dies zur Folge haben könnte, dass dieser möglicherweise in der bisherigen Form nicht oder nicht mehr eingesetzt werden kann, führt nicht zu einer Gefährdung der öffentlichen Sicherheit als konkrete Gefahrenlage, sondern lediglich dazu, dass dieses Instrument als Ermittlungsmethode in dieser Form,

wie sie vorliegend vereinbart worden ist, ausfällt. Dass diese Ermittlungsmethode aktuell zur Abwehr einer konkreten Gefahrenlage eingesetzt wird, hat das Bundeskriminalamt nicht dargetan; eine konkrete Darlegung, inwieweit ein zukünftiger Einsatz des Instrumentariums eine konkrete Gefahrenlage abwehren könnte, ebenfalls nicht. In diesem Fall liegt auch keine konkrete Gefahr vor.“

<https://www.rv.hessenrecht.hessen.de/bshe/document/LARE190035030>

Die von mir angefragte Informationen führen nicht „zu einer Änderung des Verhaltens der/des polizeilichen Gegenüber/s“. Jedes „Gegenüber“, dass sein Verhalten an den Einsatz von Quellen-TKÜ und Online-Durchsuchung durch das BKA anpassen will, kann das bereits heute auf Basis der bereits öffentlichen Informationen tun. Kein „Gegenüber“ braucht dafür die Informationen aus diesem IFG-Antrag.

Vor diesem Hintergrund ist es nicht nachvollziehbar, welche nachteiligen Auswirkungen das Bekanntwerden der Information auf Belange der inneren oder äußeren Sicherheit haben soll oder wie das Bekanntwerden der Information die öffentliche Sicherheit gefährden soll. § 3 Nr. 1 c) und § 3 Nr. 2 IFG greifen nicht.

Die Berufung auf § 3 Nr. 4 IFG verwirrt. Sie sagen nicht, ob das Dokument als Verschlusssache eingestuft ist, auch nicht mit welchem Geheimhaltungsgrad. Darüber hinaus ist eine reine Einstufung als Verschlusssache nicht ausreichend.

Das führt auch das VG Wiesbaden in seinem Urteil aus (6 K 687/15.WI): „Soweit sich die Beklagte auf § 3 Nr. 4 IFG (Geheimnis) beruft, erkennt diese selbst bereits im Widerspruchsverfahren, dass die Kennzeichnung ‚VS - NfD‘ nicht zu einer Auskunftsverweigerung führt. Insoweit reicht die formelle Einstufung als Verschlusssache vorliegend nicht aus. Begründungen, warum nicht zu veröffentlichende Punkte materiell die Einstufung als Verschlusssache rechtfertigen, hat das Bundeskriminalamt nicht vorgetragen. Es fasst die Ablehnungsgründe vielmehr in toto zusammen in § 3 Nr. 1c Nr. 2 und Nr. 4 IFG. Jeder Ausschlussgrund ist jedoch für sich selbst zu betrachten. Dezidierte Gründe, welche der Streichungen materiell die Einstufung als Verschlusssache rechtfertigen, wurden weder schriftsätzlich noch in der mündlichen Verhandlung vorgetragen. Der wohl von dem Bundeskriminalamt vorgenommene Umkehrschluss, alles was unter § 3 Nr. 1c IFG (Belange der inneren und äußeren Sicherheit) und § 3 Nr. 2 IFG (Bekanntwerden der Informationen, die die öffentliche Sicherheit

gefährden kann) falle, führe auch zur Verschlussache, lässt sich aus dem Gesetz nicht herleiten. Belange der inneren oder äußeren Sicherheit führen gerade nicht automatisch zu einer Verschlussache. Diese zu bestimmen, obliegt vielmehr der zuständigen Behörde anhand objektiver Kriterien. Mithin liegt zur Überzeugung des Gerichtes kein Verweigerungsgrund des § 3 Nr. 4 IFG vor.“

<https://www.rv.hessenrecht.hessen.de/bshe/document/LARE190035030>

Ich bitte daher erneut um Übersendung des Dokuments. Was sie schwärzen dürfen und was nicht, hat das VG Wiesbaden in bereits zwei Urteilen ausführlich dargelegt.

Ich würde mich freuen, wenn wir diesen Sachverhalt diesmal ohne Gerichtsverfahren klären können. Das spart uns und ihnen Zeit, Geld und Nerven.

Mit freundlichen Grüßen

Andre Meister