Nico Sander
RECHTSANWALT
MEDIATOR

Nico Sander Sternstraße 102, 20357 Hamburg

Verwaltungsgericht Wiesbaden
Mainzer Straße 124
65189 Wiesbaden
Per beA.

T + 49 (0)40 4143 58766
F + 49 (0)40 3567 69 87
M + 49 (0)17 9437 46 82
Threema: BTFK7ZE4

Sternstraße 102
20357 Hamburg

info@sander.legal
www.sander-law.com

Mitglied im AnwaltVerein

Bankverbindung:

DE 05 1101 0100 2282 3888 21.
SOBKDEBBXXX

Umsatzsteuer-ID:

46/207/03791

22. August 2023
Az.: AM ./. BKA-23-V

6 K 229/23

In dem Rechtsstreit

Andre Meister ./. Bundesrepublik Deutschland

wegen: Auskunft nach dem Informationsfreiheitsgesetz

wird auf den Schriftsatz der Beklagtenvertretung vom 5. Juni 2023 wie folgt erwidert:

I.
Die von dem israelischen Unternehmen NSO Group angebotene Software „Pegasus“ ist eine sogenannte Spyware, die der Hersteller nach eigenen Angaben ausschließlich an staatliche Stellen vermarktet. Mit Hilfe von „Pegasus“ können Endgeräte ausgespäht werden, auf denen die Betriebssysteme iOS oder Android laufen. „Pegasus“ kann auf alle Daten zugreifen, die auf einem infiltrierten Gerät verarbeitet werden, verschiedene Systemfunktionen wie etwa eingebaute Mikrofone zur Datenerhebung aktivieren und die gewonnenen Daten über das Internet weiterleiten.

1. Amnesty International veröffentlichte im Juli 2021 einen Bericht über Spuren erfolgter „Pegasus“-Angriffe auf iOS- und Android-basierte Smartphones und über technische Verfahren zur Aufdeckung solcher Angriffe,

s. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus.

Der Einsatz von „Pegasus“ durch verschiedene Staaten erfuhr in der Folge große mediale und politische Aufmerksamkeit.

Im Jahr 2020 erhielten Amnesty International und die Medienorganisation Forbidden Stories eine Liste mit mehr als 50.000 Telefonnummern, die als Ziele für Einsätze der Software benannt worden waren.

In der Folge schlossen sich 17 Redaktionen aus verschiedenen Ländern zu einem Netzwerk (Pegasus-Projekt) zusammen, um die erhaltenen Informationen auszuwerten und weitere Erkenntnisse zu recherchieren. Die projektbezogenen Internetauftritte der deutschen Projektpartner sind abrufbar unter

https://www.sueddeutsche.de/projekte/artikel/politik/pegasus-project-die-uebersicht-e642044;
https://www.zeit.de/schwerpunkte/pegasus-project;
https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-projekt-103.html.

Im März 2022 setzte das Europäische Parlament einen Untersuchungsausschuss zum Einsatz von „Pegasus“ und ähnlicher Überwachungs- und Spionagesoftware ein, der dem Europaparlament im Mai 2023 seinen Bericht vorgelegt hat, welcher auf der Internetpräsenz des Untersuchungsausschusses unter nachfolgender URL abrufbar ist:

https://www.europarl.europa.eu/committees/de/pega/home/highlights;
der Bericht ist abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.

Grund für die hohe Aufmerksamkeit war, dass nach den Rechercheergebnissen des Pegasus Projekts die NSO die Software an zahlreiche Staaten weltweit geliefert hat, darunter auch autoritär regierte Staaten, die mit Hilfe von „Pegasus“ Aktivisten, Oppositionelle oder Journalisten überwacht haben.

Beispielsweise waren Geräte mehrerer Personen aus dem Umfeld des 2018 im saudischen Konsulat in der Türkei ermordeten saudischen Journalisten Jamal Khashoggi infiltriert worden.

Zudem befanden sich unter den bekannt gewordenen Telefonnummern von Zielpersonen etwa die Telefonnummern von mehr als 180 Journalistinnen und Journalisten, von politischen Aktivistinnen und Aktivisten sowie von mehreren aktuellen oder ehemaligen Staats- und Regierungschefs, unter anderem Nummern des französischen Präsidenten Emmanuel Macron und des früheren französischen Premierministers Edouard Philippe. Der mexikanische Reporter Cecilio Pineda wurde ermordet, nachdem seine Nummer in den Wochen zuvor wiederholt als Ausspähziel ausgewählt worden war. In Mexiko wurden Familienmitglieder und Mitgliedern eines internationalen Ermittlungsteams hinsichtlich der 2014 in Mexiko entführten und hochwahrscheinlich ermordeten 43 Lehramtsstudenten ausgespäht.

> siehe https://www.sueddeutsche.de/projekte/artikel/politik/pegasus-project-cyberangriff-auf-die-demokratie-e519915.
> https://www.bbc.com/news/world-latin-america-40567277

Teilweise sollen ausländische Machthaber „Pegasus“ auch zu privaten Zwecken eingesetzt haben. So setzte der Emir von Dubai einem Bericht der Süddeutschen Zeitung zufolge die Spyware zur Ausspähung seiner ehemaligen Frau und deren Rechtsanwalt im Rahmen eines Sorgerechtsstreits ein.

> s. https://www.sueddeutsche.de/politik/pegasus-projekt-dubai-emir-nso-1.5432820.

2. Die Bundesregierung hat in ihrer Antwort auf eine Kleine Anfrage ausgeführt, dass die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) seit 2018 mit Vertretern der NSO Group Technologies Limited in Kontakt stehe, 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. (s. BT-Drs. 19/32246, S. 5.)

Diversen Medienberichten zufolge hat u.a. der BND „Pegasus“ erworben und die Software gegen Personen im Ausland eingesetzt, ohne dass das Parlamentarische Kontrollgremium des Bundestages hierüber informiert worden sei,

> siehe bspw.:
> https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-107.html;
> https://www.zeit.de/politik/deutschland/2021-10/pegasus-spionage-software-bnd-kaeufer-einsatz-israel?;
> https://www.sueddeutsche.de/politik/pegasusprojekt-nso-pegasus-bundesnachrichtendienst-1.5433974.

Im Rahmen und infolge des Pegasus Projekts wurden Artikel veröffentlicht, die Einzelheiten zum Ankauf von Pegasus durch das BKA beinhalten. So habe das BKA erstmals an einem Montag, Ende Oktober 2017, mit NSO verhandelt und sich von einer Delegation der NSO die Fähigkeiten der Spyware vorführen lassen. Die bei dem Treffen ebenfalls anwesenden Juristen des BKA hätten Bedenken angesichts der möglichen Totalausspähung geäußert haben. Ende 2019 soll gleichwohl nach einer Veröffentlichung der Zeit eine Handlungseinigkeit begründet worden sein.
Die NSO habe zuvor sehr intensiv um Deutschland als Kunden geworben und einen außergewöhnlich hohen Rabatt angeboten. Der Preis sollte nur 5 Millionen Euro betragen; während Mexiko über 30 Mio. Dollar für die Software bezahlte und Saudi-Arabien 55 Mio. Euro.

> s. https://www.spiegel.de/netzwelt/netzpolitik/bka-hat-umstrittene-ueberwachungssoftware-von-nso-gekauft-a-8c8039a4-a8d5-49a3-8a4b-afdf98fd165a;
> https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-nso-israel-bundeskriminalamt-kauf-innenausschuss-bundestag-unterrichtung
> https://www.zeit.de/politik/2023-05/spyware-pegasus-deutsche-behoerden-investigativpodcast.

In Bezug auf das BKA kam der Untersuchungsausschuss PEGA in seinem Abschlussbericht zu dem Ergebnis, das BKA habe eine angepasste Version der Software Pegasus von NSO erworben. Die damalige Vizepräsidentin des BKA Martina Link habe den Kauf gegenüber dem Innenausschuss des Bundestags bestätigt

> s. S. 97 des Abschlussberichts, abrufbar unter:
> https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.

Das BKA hat sich - anders als von der Beklagten dargestellt - in der Vergangenheit über spezifische Produkte zur Quellen-TkÜ aus dem Bereich der kommerziellen Software eingelassen.

> siehe etwa bzgl. FinFisher:
> https://fragdenstaat.de/blog/2022/08/02/wir-haben-das-bka-verklagt-und-gewonnen/
> sowie bereits *https://netzpolitik.org/2013/bestatigt-deutsche-behorden-haben-staatstrojaner-finfisher-fur-150-000-euro-gekauft/*;).

Zudem gab der Staatssekretär Klaus Vitt auf eine schriftliche Frage des Abgeordneten Dr. Konstantin von Notz im Jahr 2018 darüber Auskunft, dass im polizeilichen Aufgabenbereich das Forensik-Tool "Cellebrite" verwendet wird. (s. BT-Drucksache 19/3762 S. 28)

3. Laut eines Berichts des Bundesamts für Sicherheit in der Informationstechnik (BSI) verwendet Pegasus sog. Zero-Day-Exploits, für den Zugriff auf das Zielendgerät. Dabei handelt es sich um nicht veröffentlichte und dem Hersteller des Endgeräts oder der darauf befindlichen Software nicht bekannte Sicherheitslücken.

Die Wirkungsweise der Software, genauer die Schwachstellen, die das Pegasus-Programm ausnutzt, sind bislang der Öffentlichkeit nicht bekannt.

> Siehe hierzu etwa:
> https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-234348-1032.pdf?__blob=publicationFile&v=3, S. 2).

Staatstrojaner wie Pegasus sind kein statisches Produkt, sondern werden permanent angepasst und aktualisiert. Das BSI geht davon aus, dass die NSO Group ständig nach neuen Exploits für unterschiedliche Plattformen sucht.

IT-Sicherheitsmaßnahmen gegen Überwachungsmaßnahmen werden nicht gegen eine bestimmte Spyware vorgenommen, sondern gegen die Maßnahme insgesamt (z.B. Quellen - TKÜ/Online-Durchsuchung).

Das zeigt sich auch in dem von der Beklagten genannten Online-Artikel "Was hilft gegen Staatstrojaner". Der Verfasser des Artikels Moritz Tremmel hat auf eine entsprechende Anfrage des Klägers anlässlich des Vortrags der Beklagten das folgende mitgeteilt:

"Der von mir auf Golem.de veröffentlichte Artikel "Was hilft gegen den Staatstrojaner" gibt einen allgemeinen Überblick, wie man sich vor Staatstrojanern schützen kann. Der Artikel konstatiert: "Letztlich handelt es sich beim Staatstrojaner schlicht um eine Schadsoftware, die von Behörden eingesetzt wird. Entsprechend unterscheiden sich die Installationswege nicht sonderlich von gewöhnlicher Malware."

Als Beispiele werden im Artikel deshalb nicht nur bekannte Staatstrojaner herangezogen, sondern auch Malware wie Emotet, welche das BSI als "König der Schadsoftware" betitelt hatte.

Auch die im Artikel vorgestellten Schutzmaßnahmen gelten allgemein und sollen nicht nur gegen Staatstrojaner, sondern auch gegen andere Schadsoftware schützen können.

Die Sicherheitstipps sind deshalb unabhängig von einer spezifischen Software, die durch das BKA eingesetzt wird, gültig.

Zum Zeitpunkt der Veröffentlichung des zitierten Artikels war zudem nicht öffentlich bekannt, dass das BKA die Schadsoftware Pegasus einsetzt, dennoch ist der Trojaner ein Beispiel unter vielen im Artikel.

II.

Die zulässige Klage ist begründet.

Dem Informationsanspruch steht keiner der in §§ 3 - 6 IFG genannten Ausschlussgründe entgegen.

Die Darlegungslast für das Vorliegen von Ausschlussgründen liegt bei der Behörde. Dabei müssen die Angaben zwar nicht so detailliert sein, dass Rückschlüsse auf die geschützte Information möglich sind, sie müssen aber so einleuchtend und nachvollziehbar sein, dass das Vorliegen von Ausschlussgründen geprüft werden kann (vgl. BVerwG, Urteil vom 21.03.1986 – C 71/83, Rn. 15; VG Berlin, Urteil vom 10.09.2008 – 2 A 167/06; Urteil vom 26.06.2009 – 2 A 62/08, Rn. 26). Grundsätzlich muss für jede Textpassage - mitunter Wort für Wort - einzeln begründet werden, weswegen die Behörde vom Vorliegen eines Ausschlussgrundes ausgeht.

Mit ihrer Vorgehensweise, schon offen zu lassen, ob die vom Kläger begehrten amtlichen Informationen überhaupt bei ihr vorliegen oder nicht, genügt die Beklagte dieser Darlegungslast bereits im Ansatz nicht.

Im Übrigen ist hinsichtlich der einzelnen geltend gemachten Ausschlussgründe zu berücksichtigen:

1. Keine nachteilige Auswirkungen auf internationale Beziehungen (§ 3 Nr. 1 lit. a IFG)

Das Bekanntwerden der Informationen kann entgegen der Auffassung der Beklagten keine nachteiligen Auswirkungen auf internationale Beziehungen haben, gemäß § 3 Nr. 1 lit. a IFG.

Die Beklagte geht von einem fehlerhaften Sachverhalt aus **(a)**. Darüber hinaus und unabhängig davon, gelingt es der Beklagten nicht, nachteilige Auswirkungen für internationale Beziehungen fehlerfrei und nachvollziehbar zu prognostizieren **(b)**.

a) Dass ein Ankauf von Pegasus durch das BKA stattgefunden hat, ist in der Öffentlichkeit lange bekannt (s. o. Ziffer I Nr. 1). Dies gilt bereits aufgrund der vielfältigen und überregionalen Presseberichterstattung diverser renommierter Medien zu dem Thema, deren Richtigkeit von der Beklagten zu keinem Zeitpunkt in Zweifel gezogen worden ist.

Anders als die Beklagte behauptet, gibt es darüber hinaus auch offizielle Bestätigungen hierüber.

Zum einen hat die Bundesregierung im Rahmen einer Kleinen Anfrage zwar nicht den Ankauf, aber doch das Führen von Gesprächen mit dem Softwarehersteller NSO Group, um dessen Eignung für eine mögliche Verwendung durch die Sicherheitsbehörden des Bundes zu evaluieren, bestätigt (BT-Drs. 19/32246, S. 4).

Der Ankauf wiederum wurde vom BKA selbst, nämlich von der damaligen Vizepräsidentin Martina Link, gegenüber dem Innenausschuss bestätigt, worauf der Abschlussbericht des Untersuchungsausschusses PEGA Bezug nimmt.

> **s. S. 97 des Abschlussberichts, abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf.**

Ferner hat der Bundestagsabgeordnete und Mitglied des Innenausschusses Uli Grötsch den Ankauf bestätigt. Ob er an der in Rede stehenden Sitzung teilgenommen hat, ist aufgrund seiner Mitgliedschaft im Innenausschuss unbeachtlich. Aufgrund dieser Stellung ist es jedenfalls äußerst unwahrscheinlich, dass er -ggf. auch abseits von etwaigen Sitzungen- keine Kenntnis von deren Inhalten erhielt und im Übrigen auch generell über die Inhalte der Sitzungen nicht informiert wäre. Jedenfalls stellt seine Äußerung eine offizielle Äußerung dar.

Unabhängig davon, dass - wie vorgetragen - auch das BKA selbst den Ankauf bestätigt hat, wäre es mit dem Sinn und Zweck des Informationsfreiheitsgesetzes unvereinbar, dürfte die Behörde im Rahmen ihrer Prognoseentscheidungen nur von Tatsachen ausgehen, die sie „selbst schafft", indem sie Medienberichte bestätigt oder leugnet. Ansonsten läge es im Ergebnis in der Hand der Behörde, das Vorliegen der Voraussetzungen des § 3 Nr. 1 lit. a IFG zu schaffen, was wiederum dazu führen würde,

dass die Vorschrift die Wirkung einer eigentlich unzulässigen Bereichsausnahme entfalten würde. (vgl. Schoch, IFG, 2. Aufl. 2016 § 3 Rn. 35 m.w.N.)

Selbst wenn man insofern eine qualitative Unterscheidung zwischen Medienberichten und Aussagen von offizieller Seite treffen will, darf als offizielle Stelle jedenfalls nicht ausschließlich die informationspflichtige Stelle selbst gelten.

b) Selbst wenn man unterstellt, die Beklagte wäre von einem zutreffenden Sachverhalt ausgegangen, hat sie jedenfalls keine nachteiligen Auswirkungen der Bekanntgabe der angefragten Information auf diplomatische Verhältnisse plausibel darlegen können.

aa) Grundlegende Voraussetzung für die Anwendbarkeit des Ausschlussgrundes gemäß § 3 Nr. 1 lit a) IFG ist, dass die Grenzen des rein Nationalen überschritten werden und der Bereich des Auswärtigen betroffen ist (vgl. BVerwG, Urteil vom 29.06.2016 - 7 C 32.15 Rn. 10 und Rn. 30). „Nachteil" im Sinne dieser Bestimmung ist alles, was den *außenpolitischen Zielen* und der zu ihrer Erreichung verfolgten *außenpolitischen Strategie* abträglich ist. Ob ein Nachteil für die Beziehungen der Bundesrepublik Deutschland zu einem auswärtigen Staat eintreten kann, hängt wiederum davon ab, welche außenpolitischen Ziele die Bundesrepublik Deutschland *im Verhältnis zu diesem Staat* verfolgt (BVerwG, Urteil vom 29.10.2009 - 7 C 22/08 Rn. 16).

Dementsprechend geht es bei § 3 Nr. 1 lit. a IFG um Konstellationen, die Handlungen oder Dokumente anderer Staaten bzw. Völkerrechtssubjekte betreffen bzw. die Einschätzung der Bundesregierung über diese (so auch in den von der Beklagten zitierten Entscheidungen: CIA-Flüge der USA sowie ein Schreiben der Europäischen Kommission zu einem Vertragsverletzungsverfahren).

Hiervon unterscheidet sich der hiesige Fall grundlegend.

Der Abschluss eines Vertrags zwischen einem Unternehmen und einer deutschen Behörde bezüglich des Kaufs eines Produkts, das im Folgenden von einer deutschen Behörde genutzt werden soll, ist ein *rein nationaler* Sachverhalt. Ein anderer Staat ist hiervon nicht betroffen. Die Beklagte benennt auch kein konkretes außenpolitisches Ziel und keine außenpolitische Strategie, um die es hier gehen soll.

Der Vortrag der Beklagten, diplomatische Beziehungen zu anderen EU-Staaten seien gefährdet, da gegenüber diesen bei Bestätigung des Ankaufs ein Erklärungsdruck aufgebaut werde, ist nicht ausreichend, um den Sachverhalt zu einem außenpolitischen Sachverhalt zu machen. Ließe man diese Argumentation ausreichen, um nachteilige Auswirkungen auf internationale Beziehungen zu begründen, würde der Sinn und Zweck des IFG ad absurdum geführt. Denn es gibt in den verschiedensten Themenbereichen

Sachverhalte, die nicht nur in Deutschland von Relevanz, sondern in vergleichbarer Weise auch in anderen Staaten von Interesse für die Bevölkerung sind (Impfstofflieferungen, Umgang mit Versammlungen, die den Ukrainekrieg betreffen, Maßnahmen zur Erreichung der Klimaschutzziele um nur einige zu nennen). Überall dort könnte der Informationszugang unter Berufung auf vermeintlich nachteilige Auswirkungen auf internationale Beziehungen wegen eines angeblich entstehenden Erklärungsdrucks abgelehnt werden. Damit bliebe von dem grundsätzlich voraussetzungslosen Anspruch auf Informationszugang nicht mehr viel übrig.

bb) Unabhängig davon ist die These der Beklagten, dass ein Erklärungsdruck auf andere Staaten entstehe, abwegig. Es existiert keine Regelung und kein Erfahrungssatz, wonach andere EU-Staaten sich zum Kauf von Sicherheitssoftware äußern müssten, wenn ein Mitgliedstaat dies (im Rahmen der Erfüllung von Auskunftsansprüchen) tut.

Das Verhalten der Mitgliedstaaten in diesem Fall beweist gerade das Gegenteil:

Polen, Ungarn und Spanien bestätigten den Erwerb und Einsatz von Pegasus bereits ausdrücklich.

Polen gab, vertreten durch den Vizeministerpräsidenten Jaroslaw Kaczynski, in einem erstmals am 6. Januar 2022 veröffentlichten Interview zu, Pegasus von dem Unternehmen NSO gekauft zu haben, nachdem zuvor bekannt geworden war, dass die Spyware gegen polnische Journalisten, Rechtsanwälte und oppositionelle Politiker eingesetzt worden war.

> siehe hierzu bspw: https://www.euronews.com/2022/01/07/poland-s-kaczynski-admits-country-bought-pegasus-but-denies-spying-on-opponents; https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/.

Der ungarische Minister und Vizepräsident der Regierungspartei Fidesz bestätigte den Kauf und Einsatz von Pegasus im November 2021 ebenfalls.

> s. https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217)

Die ehemalige Direktorin des spanischen Geheimdienst CNI Paz Esteban bestätigte während ihrer Amtszeit ebenfalls. Die Spyware Pegasus eingesetzt zu haben gegen Teile der katalanischen Unabhängigkeitsbewegung unter anderem den ehemaligen Ministerpräsidenten Kataloniens Carles Puigdemont und seinen Nachfolger Pere Aragonès.

s. https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html;
https://www.cnbc.com/2022/05/05/separatist-politician-says-spains-spy-chief-admitted-legally-hacking-some-phones.html;
https://www.faz.net/aktuell/politik/pegasus-affaere-in-spanien-geheimdienstchefin-esteban-entlassen-18020316.html)

Obwohl die drei EU-Staaten den Ankauf des Programms also bestätigten, nahmen andere der 12 EU-Mitgliedstaaten, die nach Aussage des Softwareherstellers die Software "Pegasus" verwenden, dies nicht zum Anlass, selbst hierüber Auskunft zu geben.

Die Beklagte selbst verspürt offensichtlich keinerlei Erklärungsdruck, was das hiesige Verfahren belegt.

cc) Der Vortrag der Beklagten, Sicherheitsbehörden verpflichteten sich gegenseitig zur Vertraulichkeit über "Details der informationstechnischen Überwachung“, führt ebenfalls nicht weiter. Zum einen bringt sie keinerlei Beleg dafür, dass es eine Vertraulichkeitsabrede gibt. Es bleibt zudem unklar, was mit Details der informationstechnischen Überwachung gemeint sein soll. Naheliegend ist, dass Informationen über den Erwerb eines Softwareprodukts durch einen Staat bereits nicht darunter fallen würden. Hierfür spricht auch, dass sich deutsche Sicherheitsbehörden in der Vergangenheit bereits öffentlich in dieser Hinsicht äußerten, z.B. zur Nutzung von Forensik-Tools wie "Cellebrite" oder Spionagesoftware wie "FinFisher".

Zudem ist nicht erkennbar, inwiefern eine Vereinbarung der Beklagten mit anderen EU-Mitgliedsstaaten über den vertraulichen Umgang mit Informationen über *eigene* technische Überwachungsmaßnahmen Grundlage für deren Vertrauen in die Geheimhaltung *ausgetauschter* Informationen beeinträchtigen sollte, handelt es sich doch um diametral unterschiedliche Sachverhalte.

2. Keine nachteilige Auswirkungen auf Belange der inneren Sicherheit (§ 3 Nr. 1 lit. c IFG)

Die Einschätzung der Beklagten, durch die Bestätigung des Ankaufs von Pegasus könnten Betroffene von Überwachungsmaßnahmen entsprechende Gegenvorkehrungen treffen und somit die Handlungsspielräume des BKA einengen, ist abwegig. Wie bereits dargestellt, hat die Öffentlichkeit ohnehin bereits Kenntnis vom Ankauf der Software. Selbst wenn man dies anders sehen will, gilt dennoch das Folgende:

Das VG Wiesbaden hat jedenfalls in Bezug auf sog. Bundestrojaner festgestellt, dass gerade kein umfassender Ausschlussgrund für das klägerische Herausgabebegehren in

Bezug auf den Software-Kaufvertrag einschlägig ist. Die Beklagte hat bisher nicht plausibel dargelegt, weshalb die streitgegenständliche Interessenlage sich hiervon unterscheidet.

Schutzmaßnahmen können nicht erst dann implementiert werden, wenn von dem Einsatz einer spezifischen Software tatsächliche Kenntnis erlangt wird. Auch bei einer bloßen Vermutung können Betroffene IT-Sicherheitsmaßnahmen ergreifen. Es ist bei einer so konkreten und eindringlichen Vermutung wie im vorliegenden Fall völlig weltfremd davon auszugehen, dass Betroffene auf (weitere) Auskunft des BKA darüber warten, welche Ermittlungsmethoden sie anwenden, bevor sie versuchen hiergegen spezifische Schutzmaßnahmen ergreifen. Darüber hinaus richten sich Schutzmaßnahmen, wie in dem von der Beklagten angeführten Artikel auf www.golem.de dargestellt, nicht gegen spezifische Programme, sondern gegen Staatstrojaner und andere Schadsoftware allgemein. Jede Software, mit der eine Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung durchgeführt werden soll, muss zuvor auf dem Zielsystem installiert werden. Die technisch und sozial ansetzenden Methoden, um eine solche Installation durchzuführen, sind stets dieselben. Beispielsweise können hierzu technische Sicherheitslücken von Betriebssystemen genutzt werden, Telekommunikationsanbieter oder Hardwarehersteller zur Mitarbeit verpflichtet werden oder physisch auf das Zielsystem zugegriffen werden. Wer damit rechnet, von einer solchen Maßnahme betroffen zu sein, wird immer versuchen, sich gegen eine Infiltration möglichst gut zu sichern, einerlei welche Software möglicherweise installiert werden soll.

Insgesamt geht somit der Informationswert der Angabe, dass eine bestimmte Behörde „Pegasus“ einsetzt, für die Zielperson hinsichtlich eines möglichen Selbstschutzes gegen die Infiltration ihrer informationstechnischen Endgeräte über die allgemeine Angabe, dass diese Behörde überhaupt Online-Durchsuchungen oder Quellen-Telekommunikationsüberwachungen durchführt, nicht hinaus.

Allein die Kenntnis der konkreten Wirkungsweise der Software könnte Belange der inneren Sicherheit berühren. Dass in dem begehrten Kaufvertrag Passagen zur Wirkungsweise der Software enthalten sind, ist jedoch weder bekannt noch vorgetragen. Zudem ist auf den oben dargestellten Umstand hinzuweisen, dass es sich nach Einschätzung des BSI bei Pegasus nicht um ein statisches Produkt handelt, sondern die Software permanent angepasst und aktualisiert wird (siehe oben unter I.3). Ein Kaufvertrag aus dem Jahr 2020 wird folglich regelmäßig schon keine Auskunft darüber treffen können, welche Sicherheitslücken das Programm mittlerweile ausnutzt.

Selbst wenn aber sicherheitsrelevante Informationen über die Funktionsfähigkeit der Software in dem Vertrag enthalten sein sollten, wären diese Passagen lediglich zu schwärzen und der Vertrag im Übrigen herauszugeben. (So bspw: VG Wiesbaden, Urteil

vom 4. September 2015 – 6 K 687/15.WI –, Rn. 38 f., juris; VG Wiesbaden Urt. v. 06.05.2022, Az.: 6 K 924/21.WI S. 10 und 13.)

Die Ausführungen der Beklagten zur Person des Klägers liegen neben der Sache. Wie der Beklagten bekannt sein dürfte, handelt es sich beim Informationszugangsanspruch um einen voraussetzungslosen Anspruch. Auch das Vorliegen des Ablehnungsgrundes hängt nicht von der Person des konkreten Antragstellers ab; maßgeblich ist, ob das Bekanntwerden der Information objektiv geeignet ist, sich nachteilig auf das Schutzgut auszuwirken (BVerwG, Urteil vom 27.01.2014 - 7 C 12/13 -, juris Rn. 37 zum Gefahrenbegriff).

Zuletzt weisen wir darauf hin, dass die Beantwortung von IFG-Anträgen nicht nach Maßgabe einer wie auch immer gearteten “Transparenzstrategie” der Beklagten zu erfolgen hat, sondern allein nach Maßgabe des Gesetzes.

Der Klage ist dementsprechend stattzugeben.

Nico Sander
Rechtsanwalt