GESELLSCHAFT FÜR FREIHEITSRECHTE

Gesellschaft für Freiheitsrechte e.V. · Boyenstraße 41 · 10115 Berlin

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Graurheindorfer Str. 153
53117 Bonn

Vorab per E-Mail: poststelle@bfdi.bund.de

Berlin, den 22. September 2021

Beschwerde

1. **der Gesellschaft für Freiheitsrechte e.V., Boyenstraße 41, 10115 Berlin,**

Beschwerdeführer zu 1,

2. **des Herrn Malte Spitz, ...,**

Beschwerdeführer zu 2,

gegen

den Einsatz der Pegasus-Software durch das Bundeskriminalamt, Thaerstraße 11, 65193 Wiesbaden

Namens und in Vollmacht der Beschwerdeführer

rüge ich die Verletzung des BDSG, des BKAG, der StPO und des GG durch das Bundeskriminalamt (BKA) gemäß § 60 BDSG.

Ich rege an,

den Einsatz der Pegasus-Software durch das BKA gemäß § 16 Abs. 2 Satz 1 BDSG zu beanstanden und das BKA gemäß § 16 Abs. 2 Satz 4 BDSG zu warnen, dass ihr weiterer Einsatz voraussichtlich gegen die genannten Rechtsvorschriften verstößt.

A. Sachverhalt

I. Beschwerdeführer

Der Beschwerdeführer zu 1 ist ein gemeinnütziger Verein, der die Grund- und Menschenrechte mit juristischen Mitteln verteidigt. Dazu führt er strategische Gerichtsverfahren, geht mit Verfassungsbeschwerden gegen grundrechtswidrige Gesetze vor und bringt sich mit seiner juristischen Expertise in gesellschaftliche Debatten ein. Ein Tätigkeitsschwerpunkt des Vereins liegt im Bereich des Datenschutzes und des Schutzes gegen staatliche Überwachung. Dazu hat der Verein u.a. Verfassungsbeschwerden gegen die Ausweitung von Überwachungsbefugnissen im BKAG, in der StPO und in anderen Gesetzen erhoben, insbesondere auch gegen den Einsatz von staatlicher Spähsoftware (sog. Staatstrojaner).

Der Beschwerdeführer zu 2 ist Autor, Datenschutzberater und Generalsekretär des Beschwerdeführers zu 1. Als Autor und Aktivist beschäftigt er sich vor allem mit den Themen Datenschutz und Bürgerrechte und dem digitalen Wandel in Gesellschaft und Wirtschaft. Er ist Mitglied des Parteirates von BÜNDNIS 90/DIE GRÜNEN auf Bundesebene. In seiner Funktion als Bürgerrechtler ist er immer wieder in Kontakt mit Personen, die im Fokus der Sicherheitsbehörden stehen. Der Beschwerdeführer zu 2 besitzt ein Smartphone und kommuniziert mit Ende-zu-Ende-Verschlüsselung.

II. Einsatz der Pegasus-Software durch das BKA

Pegasus ist eine Spähsoftware, die von dem israelischen Unternehmen „NSO Group“ zum Ausspähen von iOS- und Android-Geräten entwickelt wurde. Die Software kann ohne physischen Zugriff auf den Endgeräten installiert werden und anschließend unbemerkt auf sämtliche Daten zugreifen, inklusive verschlüsselter Chats. Darüber hinaus ist die Software in der Lage, unbemerkt Kamera und Mikrofon des Geräts anzuschalten.

Den Recherchen von IT-Spezialist*innen zufolge kommt Pegasus durch drei Wege auf das Endgerät: Durch den Einsatz von verseuchten Links, durch zero-klick Infektionen oder durch Netzwerkumleitungen von IMSI-Catchern. Dabei macht sich die Software sogenannte Zero-Day-Schutzlücken, also noch unbekannte Sicherheitslücken auf den jeweiligen technischen Geräten, zunutze. Diese werden in der Regel von Hackern aufgedeckt und anschließend für viel Geld an Geheimdienste oder Unternehmen wie die NSO Group verkauft, die sie nutzen, ohne sie dem Hersteller selbst zu melden. Sobald die Pegasus-Software einmal das Handy infiltriert hat, setzt sie dort Schutzmechanismen außer Kraft und verhindert automatische Sicherheitsupdates,

> Amnesty International, Forensic Methodology Report – How To Catch NSO Group's Pegasus, 2021, abrufbar unter https://www.amnesty.org/en/documents/doc10/4487/2021/en/;
>
> Bericht auf tagesschau.de vom 18. Juli 2021, abrufbar unter https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-101.html.

Die NSO Group verkauft die Software nach eigenen Angaben nur an staatliche Stellen, unterschied dabei aber bisher nicht zwischen demokratischen und autokratischen Systemen. Zweck sei die Kriminalitäts- und Terrorismusüberwachung.

Im Juli 2021 wurde jedoch durch Recherchen von Amnesty International und einem internationalen Journalist*innenkonsortium bekannt, dass wahrscheinlich in mehreren Ländern hunderte von Journalist*innen, Menschenrechtler*innen, Rechtsanwält*innen und Oppositionellen sowie ausländischen Politiker*innen und Diplomat*innen ausgespäht wurden. Die Software wurde dabei unter anderem von Autokratien wie Saudi-Arabien, die Vereinigten Arabischen Emirate, Ruanda, Aserbaidschan und Marokko eingesetzt,

> Forbidden Stories, The Pegasus Project, alle Artikel abrufbar über https://forbiddenstories.org/case/the-pegasus-project/.

Medienberichten zufolge ließ sich das BKA 2017 über die Software informieren. Damals sei der Einsatz jedoch wegen rechtlicher Bedenken abgelehnt worden,

> ZEIT ONLINE vom 19. Juli 2021, abrufbar unter https://www.zeit.de/politik/ausland/2021-07/ueberwachungsaffaere-spionage-software-pegasus-einsatz-deutschland-bundeskriminalamt-handydaten-rechtsstaat.

Am 7. September 2021 teilten Vertreter*innen des BKA im Rahmen einer Sitzung des Innenausschusses des Bundestags mit, dass auch das BKA später eine Version dieser Software beschaffte und seit diesem Jahr einsetzt. Das Beschaffungsverfahren habe 2019 begonnen und sei 2020 abgeschlossen worden. Dabei seien keine Kontrollbehörden beteiligt gewesen. Nach Angaben des BKA wurde die Software bisher in einer mittleren einstelligen Zahl von Verfahren eingesetzt und soll auch weiterhin eingesetzt werden. Dabei werde sie sowohl zur Gefahrenabwehr als auch zur Strafverfolgung eingesetzt,

ZEIT ONLINE vom 7. September 2021, abrufbar unter
https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel.

Angaben des BKA zufolge soll die eingesetzte Version der Software einen eingeschränkten Funktionsumfang haben. So soll eine Löschfunktion für den Schutz des Kernbereichs privater Lebensgestaltung eingebaut worden sein. Zudem sollen alle Einsätze protokolliert werden. Die Telefonnummern der Zielpersonen würden „gehasht" übermittelt. Es sei zudem vertraglich vereinbart worden, dass keine sensiblen Daten an die NSO Group gehen,

ZEIT ONLINE vom 7. September 2021, abrufbar unter
https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel.

B. Rechtliche Würdigung

I. Beschwerdebefugnis

Die Beschwerdeführer sind beschwerdebefugt.

Nach § 14 Abs. 1 Nr. 6 BDSG hat sich der Bundesbeauftragte für den Datenschutz mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäß Art. 55 JI-RL zu befassen. Nicht eindeutig ist, ob in der zweiten Alternative sämtliche Voraussetzungen des Art. 55 JI-RL vorliegen müssen, oder ob es sich lediglich um eine Stelle, eine Organisation oder einen Verband im Sinne dieser Vorschrift handeln muss. Für die letztere Auffassung spricht der Wortlaut: Art. 55 JI-RL enthält eine Vertretungsregel. Würde § 14 Abs. 1 Nr. 6 BDSG umfassend auf Art. 55 JI-RL verweisen, würde es sich nicht um eine „Beschwerde einer Stelle, einer Organisation oder eines Verbandes" handeln, sondern um eine Beschwerde der betroffenen Person, die lediglich durch eine Stelle, eine Organisation oder einen Verband vertreten wird. Art. 55 JI-RL wurde mithin überschießend umgesetzt, indem Stellen, Organisationen und Verbänden im Sinne von Art. 55 JI-RL ein eigenständiges Beschwerderecht eingeräumt wurde.

Bei dem Beschwerdeführer zu 1 handelt es sich um eine Organisation im Sinne von Art. 55 JI-RL. Er hat keine Gewinnerzielungsabsicht und seine satzungsmäßigen Ziele liegen im öffentlichen Interesse. Zudem ist der Beschwerdeführer zu 1 im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig.

Sofern dem Beschwerdeführer zu 1 die Beschwerdebefugnis nach dem BDSG abgesprochen werden sollte, ist die vorliegende Beschwerde jedenfalls als Petition im Sinne von Art. 17 GG zu behandeln.

Der Beschwerdeführer zu 2 ist eine natürliche Person und potenziell von Datenverarbeitungsvorgängen im Zusammenhang mit der Pegasus-Software betroffen. Er besitzt ein Smartphone und kommuniziert mit Ende-zu-Ende-Verschlüsselung. Der Beschwerdeführer zu 2 weiß nicht, ob er Ziel einer Maßnahme wurde, bei der die Pegasus-Software eingesetzt wurde, da sowohl § 74 BKAG als auch § 101 StPO Ausnahmen von der Benachrichtigungspflicht vorsehen. Der Einsatz gegen den Kläger ist jedoch zumindest möglich. Möglich ist auch, dass die Pegasus-Software gegen Kommunikationspartner*innen des Beschwerdeführers zu 2 eingesetzt wird und er insofern von den Datenverarbeitungsvorgängen mitbetroffen ist.

Der Beschwerdeführer zu 2 wird gemäß § 14 Abs. 1 VwVfG bzw. Art. 55 JI-RL von dem Beschwerdeführer zu 1 vertreten. Auf Verlangen kann die Vollmacht schriftlich nachgewiesen werden.

II. Rechtswidrigkeit des Einsatzes der Pegasus-Software

Der Einsatz der Pegasus-Software durch das BKA ist voraussichtlich rechtswidrig. Da die genauen Spezifikationen der durch das BKA genutzten Software unbekannt sind, sind die nachfolgenden Ausführungen zwangsläufig mit Unsicherheiten behaftet. Sie erheben auch keinen Anspruch auf Vollständigkeit. Wir gehen davon aus, dass eine genaue Analyse der Software weitere Unzulänglichkeiten zu Tage befördern wird. Im Rahmen dieser Beschwerde gehen wir lediglich auf die zentralen rechtlichen Probleme ein, die mit dem Einsatz der Pegasus-Software einhergehen.

Das Outsourcing hoheitlicher Tätigkeiten verstößt gegen den Funktionsvorbehalt für Beamte (**dazu unter 1.**). Die Einbindung der privaten NSO Group verletzt zudem die Anforderungen an den Schutz gegen unbefugte Nutzung und Kenntnisnahme (**dazu unter 2.**) und an die Auftragsverarbeitung (**dazu unter 3.**). Zudem verfehlt der Einsatz der Software die gesetzlichen Anforderungen zum Schutz des Kernbereichs privater Lebensgestaltung (**dazu unter 4.**). Soweit die Software zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) eingesetzt wird, ist nicht sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird (**dazu unter 5.**). Die Software dürfte darüber hinaus unzulässige Änderungen an dem Zielsystemen vornehmen (**dazu unter 6.**). Schließlich verstößt das BKA gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektivrechtlichen Dimension, indem es Schwachstellen ausnutzt, ohne das öffentliche Interesse

ihrer Meldung an den Hersteller der betroffenen Software mit dem Interesse an der Erleichterung von Überwachungsmaßahmen gegeneinander abzuwägen (**dazu unter 7.**).

1. Unzulässiges Outsourcing hoheitlicher Tätigkeiten

Die Einbindung der privaten NSO Group in die Durchführung der Online-Durchsuchung bzw. Quellen-TKÜ verstößt gegen den Funktionsvorbehalt für Beamte gemäß Art. 33 Abs. 4 GG. Nach dieser Vorschrift ist die Ausübung hoheitlicher Befugnisse als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen.

Der Funktionsvorbehalt des Art. 33 Abs. 4 GG soll gewährleisten, dass die Ausübung hoheitsrechtlicher Befugnisse regelmäßig den für das Berufsbeamtentum institutionell garantierten besonderen Sicherungen qualifizierter, loyaler und gesetzestreuer Aufgabenerfüllung unterliegt,

> vgl. BVerfGE 130, 76 Rn. 136.

Bei der Online-Durchsuchung und der Quellen-TKÜ zu Zwecken der Gefahrenabwehr oder der Strafverfolgung handelt es sich zweifellos um hoheitsrechtliche Befugnisse.

Diese wurden der NSO Group auch teilweise übertragen. Es liegt keine bloße Verwaltungshilfe vor, bei der die NSO Group lediglich im Rahmen einer untergeordneten Tätigkeit, vorbereitend oder rein ausführend tätig wird. Die NSO Group stellt ihre Leistungen zwar in den Dienst des BKA, sie behält jedoch nach den uns vorliegenden Informationen die volle Kontrolle über die technische Infrastruktur zum Einsatz des Trojaners. Sie entscheidet über die Art und Weise des Eindringens in das Zielsystem, die Nutzung und Zurückhaltung von Sicherheitslücken, die Änderungen am Zielsystem sowie das Kopieren und Ausleiten von Daten.

Eine Ausnahme vom Funktionsvorbehalt für Beamte ist im vorliegenden Fall nicht zulässig. Die Möglichkeit von Ausnahmen ist für Fälle eingeräumt worden, in denen der Sicherungszweck des Funktionsvorbehalts die Wahrnehmung der betreffenden hoheitlichen Aufgaben durch Berufsbeamte ausweislich bewährter Erfahrung nicht erfordert oder im Hinblick auf funktionelle Besonderheiten nicht in gleicher Weise wie im Regelfall angezeigt erscheinen lässt. Je intensiver eine bestimmte Tätigkeit Grundrechte berührt, desto weniger sind Einbußen an institutioneller Absicherung qualifizierter und gesetzestreuer Aufgabenwahrnehmung hinnehmbar,

> BVerfGE 130, 76 Rn. 145 ff.

Daran gemessen ist eine Ausnahme vom Funktionsvorbehalt unzulässig. Die Online-Durchsuchung und die Quellen-TKÜ gehören zu den schwersten Grundrechtseingriffen, die das Überwachungsregime unserer Rechtsordnung kennt. Sie erfordert eine besondere Qualifikation und Gesetzestreue der tätigen Personen, die bei Privaten nicht hinreichend gewährleistet ist.

2. Unzureichender Schutz gegen unbefugte Nutzung und Kenntnisnahme

Die Einbindung der privaten NSO Group geht auch zwangsläufig mit vermeidbaren Risiken einer unbefugten Nutzung der verarbeiteten Daten einher.

Gemäß §§ 49 Abs. 2 Satz 2 und 3, 51 Abs. 2 Satz 2 BKAG und §§ 100a Abs. 5 Satz 2 und 3, 100b Abs. 4 StPO ist das für die Überwachungsmaßnahme eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen und sind die kopierten Daten nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

Diesen Anforderungen wird der Einsatz der Pegasus-Software nicht gerecht. Die Software wird nach den uns vorliegenden Informationen von der NSO Group kontrolliert und gewartet. Schon dieser Umstand begründet ein vermeidbares Risiko einer unbefugten Nutzung. Denn es ist nicht gewährleistet, dass die NSO Group die eingesetzte Software nicht für anderweitige Zwecke nutzt oder Kenntnis von den erlangten Daten nimmt. Im Rahmen der journalistischen Recherchen zu Pegasus haben Journalist*innen die Nummern der abgehörten Personen herausfinden können. Ein Zugriff Dritter war mithin möglich. Das Unternehmen gibt darüber hinaus selbst an, nachträglich prüfen zu können, ob die Software vertragsgemäß eingesetzt wurde. Dies impliziert die Möglichkeit der Kenntnisnahme von Daten durch Mitarbeiter*innen der NSO Group.

Möglich ist auch, dass die NSO Group anderen Kunden die Nutzung gewährt oder erlangte Daten weitergibt. Dabei gilt es zu beachten, dass die NSO Group als israelisches Unternehmen dem dortigen Recht unterliegt und zudem für eine Vielzahl von Staaten tätig ist, darunter Autokratien wie Saudi-Arabien, die Vereinigten Arabischen Emirate, Ruanda, Aserbaidschan und Marokko.

Möglich ist schließlich auch, dass Dritte sich unbefugt Zugriff verschaffen. Dass es sich hierbei nicht um ein abwegiges Szenario handelt, zeigt ein Vorfall, bei dem ein Mitarbeiter der NSO Group die Software genutzt haben soll, um das System einer persönlichen Bekannten zu infiltrieren. Ein anderer (ehemaliger) Mitarbeiter bestätigte gegenüber dem Magazin Motherboard, es habe nichts gegeben, das ihn davon hätte abhalten können, das System gegen wen auch immer einzusetzen. Es gebe keinen wirklichen Weg, sich dagegen zu schützen. Techniker würden immer Zugang haben.

Motherboard vom 28. April 2020, abrufbar unter https://www.vice.com/en/article/bvgwzw/nso-group-employee-abused-pegasus-target-love-interest.

Die Risiken einer unbefugten Veränderung, Löschung oder Kenntnisnahme werden dadurch erhöht, dass die erlangten Daten über Server der NSO Group geleitet werden, die in verschiedenen Ländern stehen und so dem Zugriff der NSO Group selbst und Dritter ausgesetzt sind,

vgl. Marczak/Scott-Railton/McKune/Razzak/Deibert, Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, Citizen Lab Research Report No. 113, University of Toronto, 2018, abrufbar unter https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Das BKA hat sich nach eigenen Angaben von der NSO Group vertraglich zusichern lassen, dass keine Daten an das Unternehmen abfließen. Eine solche vertragliche Zusicherung wird den Anforderungen an den Schutz des Trojaners und der mit seiner Hilfe erhobenen Daten nicht gerecht. Das mag noch für ein Unternehmen mit Sitz in Deutschland oder zumindest in der Europäischen Union in Frage kommen, das den hiesigen Datenschutzbestimmungen unterliegt und dem im Falle eines Verstoßes behördliche Verfügungen oder gar Geldbußen drohen; im Verhältnis zu Unternehmen mit Sitz außerhalb der EU ist aber Vergleichbares nicht gewährleistet.

3. Unzulässige Auftragsverarbeitung

Damit ist auch § 62 Nr. 2 BDSG verletzt. Nach dieser Vorschrift darf ein Verantwortlicher nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anordnungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

Eine vertragliche Zusicherung ist nicht ausreichend. Die Gewährleistung der Rechte der betroffenen Personen muss vielmehr auch tatsächlich sichergestellt werden. Die Sorgfaltspflichten richten sich dabei auch nach dem Gefährdungspotential für die Betroffenen und der Sensibilität der verarbeiteten Daten.

Im vorliegenden Fall gilt es zu berücksichtigen, dass hoch sensible Daten erhoben werden, die zumindest teilweise dem Kernbereich privater Lebensgestaltung zuzurechnen sind, unabhängig davon, ob diese Erhebung zulässig ist oder nicht,

vgl. zum unzureichenden Schutz auf der Erhebungsebene unten unter 4.,

Wie bereits unter 2. dargelegt, ist die Einbindung der NSO Group mit erheblichen Risiken einer unbefugten Nutzung personenbezogener Daten verbunden. Das BKA verletzt seine Auswahlverantwortung, indem es ein profitorientiertes Unternehmen, das Medienberichten zufolge auch im Auftrag autokratischer Staaten tätig ist, mit der Verarbeitung hochsensibler Daten aus der Online-Durchsuchung und Quellen-TKÜ betraut.

4. Unzureichender Schutz des Kernbereichs privater Lebensgestaltung

Nach der Rechtsprechung des Bundesverfassungsgerichts sind beim heimlichen Zugriff auf informationstechnische Systeme technische Sicherungen einzusetzen, mit deren Hilfe Informationen, die den Kernbereich privater Lebensgestaltung berühren, aufgespürt und isoliert werden können,

BVerfGE 120, 274 Rn. 281; 141, 220 Rn. 219.

Diese Vorgabe wird durch § 49 Abs. 7 Satz 2 BKAG und durch § 100d Abs. 3 Satz 1 StPO umgesetzt. Danach ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

Auch die Quellen-TKÜ weist eine besondere Kernbereichsnähe auf. Zwar ist sie nach der Rechtsprechung des Bundesverfassungsgerichts nicht in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt wie die Online-Durchsuchung. Allerdings ist auch bei der Quellen-TKÜ auf der Erhebungsstufe eine Prüfung geboten, ob die Wahrscheinlichkeit der Erfassung höchstprivater Gespräche besteht, deren Überwachung gegebenenfalls zu verbieten ist,

BVerfGE 141, 220 Rn. 237 ff.

Entsprechend legen § 51 Abs. 7 Satz 1 BKAG und § 100d Abs. 1 StPO fest, dass die Maßnahme unzulässig ist, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden.

Diesen Anforderungen genügt die Pegasus-Software nach unserer Kenntnis nicht. Nach Angaben des BKA soll in der deutschen Pegasus-Version der Schutz des Kernbereichs durch eine sofortige und separate Datenlöschung sichergestellt werden. Dies ist nicht ausreichend. Das zweistufige Schutzkonzept des Bundesverfassungsgerichts verlangt sowohl bei der Online-Durchsuchung als auch bei der Quellen-TKÜ auch Sicherungen auf der Erhebungsebene. Diese werden durch eine

nachträgliche Löschung nicht gewährleistet. Dies gilt erst recht, wenn die Daten zwischenzeitlich auf Servern eines privaten Unternehmens in verschiedenen Ländern gespeichert werden.

5. Keine Beschränkung auf laufende Kommunikation bei Quellen-TKÜ

Nach der Rechtsprechung des Bundesverfassungsgerichts ist streng zwischen der Online-Durchsuchung und der Quellen-TKÜ zu unterscheiden. Während die Quellen-TKÜ zielgerichtet die laufende Kommunikation überwacht, und mithin an Art. 10 Abs. 1 GG zu messen ist, greift die Online-Durchsuchung auf den Speicher des Zielsystems zu. Für diesen Fall entwickelte das Bundesverfassungsgericht das Grundrecht der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) aus Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG.

Das Bundesverfassungsgericht betonte die besondere Schwere dieser tief in das Privatleben eingreifenden Überwachungsmaßnahme und stellte daher insbesondere an die Online-Durchsuchung hohe Anforderungen. Eine solche ist nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen,

> vgl. BVerfGE 120, 274 Rn. 247.

Aufgrund dieser aus verfassungsrechtlichen Gründen notwendigen Unterscheidung ist eine technische Trennung zwischen der sogenannten Quellen-TKÜ und der Online-Durchsuchung erforderlich. Entsprechend verlangt § 51 Abs. 2 Nr. 1 BKAG, dass durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird.

Die Trennung zwischen Online-Durchsuchung und Quellen-TKÜ wurde in der StPO zwar auf verfassungswidrige Weise ein Stück weit aufgelöst, aber auch nach § 100a Abs. 5 Satz 1 Nr. 1 StPO ist technisch sicherzustellen, dass die Maßnahme ausschließlich die laufende Telekommunikation oder Inhalte und Umstände der Kommunikation betrifft, die ab dem Zeitpunkt der Anordnung auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können.

Die Pegasus-Software kennt die Unterscheidung zwischen Online-Durchsuchung und Quellen-TKÜ grundsätzlich nicht. Sobald sie einmal in das Endgerät eingeschleust ist, übernimmt sie dieses vollständig. Ob die nach Angaben des BKA modifizierte Version der Software tatsächlich technisch sicherstellt, dass ausschließlich laufende Telekommunikation überwacht wird, erscheint zweifelhaft und bedarf daher einer genauen Prüfung.

6. Unzulässige Veränderungen des Zielsystems

Nach § 49 Abs. 2 Satz 1, § 51 Abs. 2 Satz 2 BKAG und § 100a Abs. 5 Satz 1 Nr. 2 und 3, § 100b Abs. 4 StPO ist technisch sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und dass die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Dies dürfte beim Einsatz der Pegasus-Software nicht gewährleistet sein. Die international genutzte Version der Software hat umfassenden Zugriff auf das Zielsystem. Unter anderem ist die Software in der Lage, Kamera und Mikrofon zu aktivieren, was nach deutschem Recht unzulässig ist. Darüber hinaus legt die Software Dateien auf dem Zielsystem ab, die nach dem Einsatz nicht vollständig gelöscht werden. Nur so konnte die Infiltration vieler Geräte nachgewiesen werden.

7. Rechtswidriges Ausnutzen von Sicherheitslücken

Der Einsatz verstößt schließlich auch gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (IT-Grundrecht) in seiner objektiv-rechtlichen Dimension. Das Bundesverfassungsgericht hat hierzu in seiner Grundsatzentscheidung vom 8. Juni 2021 ausgeführt:

> *„Indessen verlangt die grundrechtliche Schutzpflicht eine Regelung darüber, wie die Behörde bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken den Zielkonflikt zwischen dem notwendigen Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung von Quellen-Telekommunikationsüberwachungen andererseits aufzulösen hat. Der Behörde muss eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine Zero-Day-Schutzlücke bekannt wird. Es ist sicherzustellen, dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, beides zueinander ins Verhältnis setzt und die Sicherheitslücke an den Hersteller meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.“*
>
> BVerfG, Beschluss des Ersten Senats vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 44.

Die Bundesregierung ist inzwischen tätig geworden und plant angeblich die Einführung eines Schwachstellenmanagements,

tagesschau.de vom 7. September 2021, abrufbar unter
https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-105.html.

Solange ein solches noch nicht implementiert ist, ist die Ausnutzung von Zero-Day-Schutzlücken unzulässig. Jedenfalls sind die jeweils zuständigen Behörden verpflichtet, die vom Bundesverfassungsgericht geforderte Abwägung zwischen Schutz der IT-Sicherheit und Erleichterung der Gefahrenabwehr bzw. Strafverfolgung selbst vorzunehmen.

Es ist nicht ersichtlich, dass dies geschehen ist. Es ist vielmehr davon auszugehen, dass die ausgenutzten Sicherheitslücken dem BKA gar nicht bekannt sind, weil die NSO Group die Kenntnisse als Betriebsgeheimnisse für sich behält. Dies entbindet das BKA selbstverständlich nicht von seiner Schutzpflicht. Vielmehr ist das BKA durch die Beauftragung der NSO Group für das Zurückhalten und Ausnutzen von Sicherheitslücken durch diese mitverantwortlich.

Bei der gebotenen Abwägung wäre Folgendes zu berücksichtigen: Die zurückgehaltenen Sicherheitslücken werden Medienberichten zufolge auch im Auftrag von autokratischen Staaten ausgenutzt, um Journalist*innen, Menschenrechtler*innen, Rechtsanwält*innen und Oppositionelle sowie ausländischen Politiker*innen und Diplomat*innen auszuspähen. Es ist davon auszugehen, dass auch Deutsche bzw. in Deutschland lebende Personen betroffen sind. Die Schäden für die Demokratie sind gravierend. Für Einzelne können die Folgen unter Umständen tödlich sein. So wird beispielsweise vermutet, dass die mittels Pegasus erfolgte Überwachung verschiedener Personen im Zusammenhang mit der Ermordung des saudischen Journalisten Jamal Khashoggi im Herbst 2018 stand,

vgl. tagesschau.de vom 18. Juli 2021, abrufbar unter
https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-saudi-arabien-101.html.

Dem steht ein geringer Mehrwert für die Gefahrenabwehr und die Strafverfolgung gegenüber. Nach Angaben des BKA bewegt sich die Anzahl der Einsätze im mittleren einstelligen Bereich. Die Abwägung müsste folglich zugunsten der Meldung der Sicherheitslücken an die Hersteller ausfallen.

Dr. Bijan Moini
Rechtsanwalt (Syndikusrechtsanwalt)