Berlin und Brüssel, 14. Oktober 2025

An
Zentral- und Ansprechstelle Cybercrime (ZAC NRW)
Staatsanwaltschaft Köln
50926 Köln
vorab per E-Mail: zac@sta-koeln.nrw.de

und

Staatsanwaltschaft Krefeld
Postfach 101055
47714 Krefeld
vorab per E-Mail: poststelle@sta-krefeld.nrw.de

und

Cybercrime-Kompetenzzentrum
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf
vorab per E-Mail: cybercrime.lka@polizei.nrw.de

Hiermit erstatten

1. MdEP Daniel Freund
   […]

   als Verletzter

und

2. die Gesellschaft für Freiheitsrechte e.V.
   Boyenstraße 41
   10115 Berlin
   vorliegend vertreten durch den Generalsekretär Malte Spitz
   Telefon: +49 30 54908100
   info@freiheitsrechte.org

Strafanzeige wegen Verstoßes gegen §§ 201 Abs. 1 Nr. 1, Abs. 2 Satz 1 Nr. 1, Abs. 4 i.V.m. 22, 23 Abs. 1 bzw. §§ 202c Abs. 1 Nr. 2, 303a Abs. 1, 2, 3, 303b Abs. 1, 3, 5 StGB sowie wegen Beihilfe gemäß § 27 StGB zu den dargestellten Straftaten

gegen

Viktor Orbán und Unbekannt.

Der Anzeigeerstatter zu 1) stellt zugleich als Verletzter Strafantrag nach § 205 StGB und § 303c StGB, sowie bezüglich aller weiterer in Frage kommender Straftatbestände.

A. Vorbemerkung

Am 27. Mai 2024 erhielt der deutsche Abgeordnete des Europäischen Parlaments Daniel Freund (im Folgenden Anzeigeerstatter zu 1)) an seine parlamentarische E-Mail-Adresse eine E-Mail von bislang unbekannten Absender*innen. Die E-Mail stammte angeblich von einer ukrainischen Studentin. Diese erbat für ein Seminar vom Anzeigeerstatter zu 1) eine kurze Nachricht. Zudem enthielt die E-Mail einen Link, bei dessen Anklicken eine Spähsoftware auf Geräte des Abgeordneten installiert worden wäre. Nach der Einschätzung von Sicherheitsexpert*innen handelte es sich dabei um ein Spähprogramm des israelischen Unternehmens „Candiru Ltd." bzw. „Saito Tech Ltd.". Der Anzeigeerstatter zu 1) klickte nicht auf den Link.

Die Spionagesoftware hätte es den Täter*innen ermöglicht, den Anzeigeerstatter zu 1) mithilfe des infiltrierten Geräts, beispielsweise seines Mobiltelefons, zu überwachen. Die Täter*innen hätten die Möglichkeit gehabt, Telefongespräche und Kommunikation auf dem infiltrierten Gerät mitzuhören und aufzuzeichnen und auf Mikrofon und Kamera des Telefons zuzugreifen, um so auch persönliche Gespräche heimlich zu belauschen und aufzunehmen.

Es ist unbekannt, wer als Täter*in für den Spähangriff zur Verantwortung zu ziehen ist. Eine Liste mit einzelnen Ermittlungsansätzen befindet sich am Ende des Dokuments. Es besteht jedoch eine hohe Wahrscheinlichkeit, dass es sich um einen Spionageangriff aus Ungarn handelt, der von der ungarischen Regierung und damit von Ministerpräsident Viktor Orbán angeordnet wurde.

Es bestehen damit tatsächliche Anhaltspunkte und der Verdacht, dass sich die noch unbekannten Täter*innen insbesondere nach §§ 201 Abs. 1 Nr. 1, Abs. 2 Nr. 1, Abs. 4 i.V.m. §§ 22, 23 Abs. 1 sowie § 202c Abs. 1 Nr. 2 StGB strafbar gemacht haben, indem sie Anstrengungen unternahmen, um die Geräte des Anzeigeerstatters zu 1) zu infiltrieren und abzuhören.

Darüber hinaus bestehen tatsächliche Anhaltspunkte und der Verdacht dafür, dass sich Mitarbeiter*innen der Saito Tech Ltd. als Herstellerin des dafür genutzten Spähprogramms insbesondere gemäß §§ 201 Abs. 1 Nr. 1. Abs. 2 Nr. 1, Abs. 4, 22, 23 Abs. 1 i.V.m. 27 Abs. 1 StGB wegen Beihilfe zur Verletzung der Vertraulichkeit des Wortes sowie ebenfalls gemäß § 202c Abs. 1 Nr. 2 StGB strafbar gemacht haben.

Zudem bestehen tatsächliche Anhaltspunkte und der Verdacht, dass der ungarische Ministerpräsident Viktor Orbán und andere ungarische Regierungsverantwortliche an den dargestellten Straftaten als Täter*innen oder Anstifter*innen beteiligt waren.

Der Verletzte und Anzeigeerstatter zu 1) stellt **Strafantrag** wegen aller verwirklichten Delikte. Wir regen die Einleitung eines Ermittlungsverfahrens wegen des strafbaren Verhaltens an.

Das Bundesministeriums des Inneren hat Betroffenen von Angriffen mit Spyware aus dem Ausland ausdrücklich empfohlen, Strafanzeige zu erstatten,

> so Andreas Könen (Abteilungsleiter „Cyber- und IT-Sicherheit" im BMI a.D.) in der Sitzung des Ausschusses für Digitales am 27. November 2023, in der der EU-Untersuchungsbericht zu Spähsoftware „Pegasus" diskutiert wurde (https://www.bundestag.de/mediathek/video?videoid=7578795, ab Minute 00:39:54, abgerufen am 14. Oktober 2025).

Zum Schutz der Betroffenen ist von hoher Bedeutung, dass die Täter*innen und Teilnehmenden an solchen Angriffen ermittelt und Strafverfahren gegen diese eingeleitet werden.

Staatliche Stellen müssen die Grundrechte, insbesondere das Fernmeldegeheimnis (Art. 10 GG) und das IT-Grundrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), auch vor Eingriffen aus dem Ausland, beispielsweise durch ausländische Geheimdienste schützen,

> BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18, Rn. 26 ff., 30 ff., 33; BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17, Rn. 248 ff.

B. Sachverhalt im Einzelnen

I. Zu den Anzeigeerstatter*innen

Der Anzeigeerstatter zu 1) ist Mitglied des Europäischen Parlaments und der dortigen Fraktion Die Grünen/EFA.

In dieser Funktion setzt er sich für Demokratie und Rechtsstaatlichkeit in Europa ein, gerade auch mit Blick auf Ungarn. Er äußert sich öffentlich und insbesondere in Redebeiträgen im Europäischen Parlament kritisch gegenüber der von Viktor Orbán geführten ungarischen Regierung,

> beispielsweise in einer Pressekonferenz am 23. November 2023 https://multimedia.europarl.europa.eu/en/webstreaming/20231023-1300-SPECIAL-PRESSER; https://euractiv.de/news/eu-gelder-an-ungarn-europaeisches-parlament-will-kommission-verklagen/ vom 16. Januar 2024 (abgerufen am 14. Oktober 2025); Redebeiträge beispielsweise am 21. November 2023 (Continuing threat to the rule of law, the independence of justice and the non-fulfilment of conditionality for EU funding in Hungary (debate)) siehe ab 20:39 CET https://multimedia.europarl.europa.eu/en/webstreaming/20231121-0900-PLENARY?seekTo=231121203950 ; am 17. Januar 2024 (Conclusions of the European Council meeting of 14-15 December 2023 and preparation of the Special European Council meeting of 1 February 2024 - Situation in Hungary and frozen EU funds (joint debate – European Council meetings)) siehe ab 10:16 CET https://multimedia.europarl.europa.eu/en/webstreaming/20240117-0900-PLENARY?seekTo=240117101603; am 28. Februar 2024 (Report on the Commission's 2023 Rule of Law report (debate)) https://multimedia.europarl.europa.eu/en/webstreaming/20240228-0900-PLENARY?seekTo=240228170722 ab 17:07 CET (jeweils abgerufen am 14. Oktober 2025).

In den Monaten vor dem Angriff hatte der Einsatz des Anzeigeerstatters zu 1) erheblichen Einfluss darauf, dass der Rat aufgrund eines Kommissionsvorschlags die Anwendung der Verordnung 2020/2092 über eine allgemeine Konditionalitätsregelung zum Schutz des Haushalts der Union („Konditionalitätsverordnung") und damit Sanktionen gegen Ungarn beschloss,

> https://www.spiegel.de/politik/deutschland/europaeisches-parlament-daniel-freund-und-moritz-koerner-zwei-gegen-ursula-von-der-leyen-a-f975dfe6-20a2-41eb-9882-6e292d8c5111 (abgerufen am 14. Oktober 2025).

Als Viktor Orbán selbst im Plenum des Europaparlaments am 9. Oktober 2024 die Ziele seiner Ratspräsidentschaft vorstellte, sprach er in seiner Antwort den Anzeigeerstatter zu 1) direkt an, machte ihm unbelegte Vorwürfe, insbesondere der Korruption,

> siehe Minute 07:05 von 13:47 in der Aufzeichnung der europäischen Parlaments https://multimedia.europarl.europa.eu/en/video/presentation-of-the-programme-of-

activities-of-the-hungarian-presidency-closing-statements-by-maros-sefcovic-european-green-deal-interinstitutional-relations-and-foresight-and-by-viktor-orban-hungarian-prime-minister_I261580 (abgerufen am 14. Oktober 2025).

Bei allen Entgegnungen auf Vorwürfe von Abgeordneten ist der Anzeigeerstatter zu 1) der einzige, den Orbán mit Namen anspricht.

Durch seine berufliche Tätigkeit steht der Anzeigeerstatter mit zahlreichen Menschen in Kontakt, die sich ebenfalls für Rechtsstaatlichkeit in Europa und insbesondere in Ungarn engagieren.

Die Anzeigeerstatterin zu 2) ist ein gemeinnütziger Verein, der die Grund- und Menschenrechte mit juristischen Mitteln verteidigt. Dazu führt sie strategische Gerichtsverfahren, geht mit Verfassungsbeschwerden gegen grundrechtswidrige Gesetze vor und bringt sich mit ihrer juristischen Expertise in gesellschaftliche Debatten ein. Ein Tätigkeitsschwerpunkt der Anzeigeerstatterin zu 2) liegt im Bereich des Datenschutzes und des Schutzes gegen staatliche Überwachung.

II. Zum Anbieter der Spähprogramme und -services („Candiru Ltd.“)

Das Unternehmen, das die im konkreten Falle genutzte Software „Candiru“ anbietet und herstellt, wurde 2014 als „Candiru Ltd.“ in Tel Aviv gegründet und seitdem mehrfach umbenannt. Auch wenn das Unternehmen gegenwärtig „Saito Tech Ltd.“ heißt,

https://pitchbook.com/profiles/company/437928-67#overview sowie https://www.business-humanrights.org/en/companies/candiru/ und https://utoronto.scholaris.ca/server/api/core/bitstreams/3e255059-7679-48b7-b84a-f5de13929dfc/content, S. 2 (jeweils abgerufen am 14. Oktober 2025),

wird weiterhin der ursprüngliche Name in Artikeln und Forschungsberichten verwendet, weswegen auch im Folgenden der ursprüngliche Name verwendet wird.

Die Häufigkeit der Namensänderung scheint Teil einer bewusst intransparenten Unternehmensstruktur zu sein,

https://utoronto.scholaris.ca/server/api/core/bitstreams/3e255059-7679-48b7-b84a-f5de13929dfc/content, S. 2 (abgerufen am 14. Oktober 2025).

Über das Unternehmen und seine Produkte ist wenig bekannt. Das Unternehmen hat keine eigene Webseite und keine Hinweisschilder an seinem Geschäftssitz. Seine Arbeitnehmer*innen machen ihre Positionen nicht auf LinkedIn oder sonstigen Kanälen öffentlich,

https://www.haaretz.com/middle-east-news/2019-01-04/ty-article/.premium/top-secret-israeli-cyberattack-firm-revealed/0000017f-e36d-d38f-a57f-e77ff84b0000 (abgerufen am 14. Oktober 2025).

Vertragspartner*innen der „Candiru Ltd.“ sind ausschließlich Regierungen,

https://utoronto.scholaris.ca/server/api/core/bitstreams/3e255059-7679-48b7-b84a-f5de13929dfc/content, S. 1 (abgerufen am 14. Oktober 2025).

Unter den Kund*innen befindet sich auch Ungarn,

https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/, S. 7 (abgerufen am 14. Oktober 2025).

Weitere bekannt gewordene Kund*innen sind u.a. Usbekistan, Saudi Arabien, die Vereinigten Arabischen Emirate, Spanien und Singapur,

https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit; https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/, S. 7 (abgerufen am 14. Oktober 2025), https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ (abgerufen am 14. Oktober 2025).

Damit sind unter den Kund*innen auch solche Staaten, die Spionagesoftware bereits rechtsstaatswidrig eingesetzt haben. Laut Amnesty International waren beispielsweise Saudi-Arabien, Ungarn und die Vereinigten Arabischen Emirate Kund*innen der NSO-Group und nutzten deren Spionagesoftware „Pegasus“ zu rechtswidrigen Zwecken

https://www.amnesty.at/news-events/news/pegasus-projekt-in-zusammenarbeit-mit-amnesty-aktivist-innen-journalist-innen-und-politiker-innen-weltweit-mit-nso-spyware-ausgespaeht/ (abgerufen am 14. Oktober 2025).

Bekannt geworden ist, dass Saudi-Arabien die Spionagesoftware „Pegasus“ gegen den oppositionellen saudischen Journalisten Jamal Khashoggi und ihm nahestehende Personen eingesetzt hat,

dazu https://www.amnesty.at/news-events/news/pegasus-projekt-in-zusammenarbeit-mit-amnesty-aktivist-innen-journalist-innen-und-politiker-innen-weltweit-mit-nso-spyware-ausgespaeht/ und https://www.zeit.de/politik/2023-04/jamal-khashoggi-journalist-pegasus-investigativpodcast (jeweils abgerufen am 14. Oktober 2025).

Ebenso wurde Spionagesoftware auch gegen die saudische Frauenrechtsaktivistin Loujain al-Hathloul eingesetzt,

https://www.zeit.de/politik/ausland/2021-07/spionage-software-pegasus-cyberwaffe-ueberwachung-menschenrechte-enthuellung/seite-3 (abgerufen am 14. Oktober 2025).

Es bestehen keine Erkenntnisse, dass Verträge durch die „Candiru Ltd.“ wegen solcher Vorfälle widerrufen bzw. beendet wurden. Vielmehr scheinen Verträge auch in Kenntnis solcher Vorkommnisse geschlossen zu werden, da beispielsweise gegen Saudi-Arabien bereits seit 2014 (Gründungsjahr der „Candiru Ltd.“) Vorwürfe des rechtsstaatswidrigen Einsatzes von Spionagesoftwares geäußert werden,

https://www.hrw.org/de/news/2014/06/27/saudi-arabien-spionage-app-entdeckt (abgerufen am 14. Oktober 2025).

Ob deutsche Behörden Angebote der „Candiru Ltd.“ nutzen, ist unbekannt,

eine diesbezügliche schriftliche Frage an die Bundesregierung vom 13. September 2021 durch die Abgeordnete Martina Renner blieb unbeantwortet, BT-Drucksache 19/32490, Frage 39, S. 27.

Das Unternehmen befindet sich seit dem 4. November 2021 auf der Liste des US-amerikanischen Handelsministeriums für Unternehmen, deren Aktivitäten der nationalen Sicherheit oder außenpolitischen Interessen der USA zuwiderlaufen (*Entity List for engaging in activities that are contrary to the national security or foreign policy interests of the United States*),

https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list (abgerufen am 14. Oktober 2025).

„Candiru Ltd." ist auf dieser Liste wegen schädlicher Cyber-Aktivitäten (*„malicious cyber activities*") verzeichnet. Dem Ministerium lagen Beweise vor, wonach „Candiru Ltd." Spähprogramme hergestellt und an Staaten verkauft hat, welche diese Programme für Angriffe auf Regierungsmitarbeiter*innen, Journalist*innen, Aktivist*innen und insbesondere auch auf Dissident*innen im Exil nutzen. Das US-amerikanische Handelsministerium sprach dabei von transnationaler Repression als Praxis autoritärer Regime, welche die internationale Ordnung gefährdet,

https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list (abgerufen am 14. Oktober 2025).

III. Zu den Angeboten der „Candiru Ltd."

Die „Candiru Ltd." bietet weitgehende Cyberspionage an. Mittels Spionagesoftware können Netzwerke und Geräte infiltriert und ausgespäht werden. Die Spähprogramme können mittels verschiedener Vektoren wie malicious links, man-in-the-middle attacks und physical attacks installiert werden – aber möglicherweise auch über einen zero-click-vector, bei dem keinerlei Mitwirkung der Betroffenen notwendig ist,

https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf, S. 3 (abgerufen am 14. Oktober 2025).

Malicious links (auch malware URLs genannt) können via E-Mails verschickt werden. Klickt die empfangende Person auf den Link, wird automatisiert eine Schadsoftware heruntergeladen und installiert, die den Angreifer*innen Zugriff auf das Gerät verschafft, sodass Daten abgegriffen werden können.

Die Installation erfolgt vollautomatisiert in mehreren Schritten,

https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#exploit-techniques (abgerufen am 14. Oktober 2025).

Welche Art von Eingriffen mit der Software möglich sind, kann einer geleakten Produktbeschreibung eines Angebots entnommen werden,

https://web.archive.org/web/20200905040710/https://www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf#page=1 (abgerufen am 14. Oktober 2025).

Das Angebot führt aus, dass die Spähprogramme auf private Daten aus einer Reihe von Apps und Accounts wie Gmail, Skype, Telegram oder Facebook zugreifen können. Darüber hinaus können Browserverlauf und Passwörter abgegriffen und Fotos von dem Bildschirm gemacht werden. Auch Webcam und Mikrofon des anvisierten Geräts können jederzeit angeschaltet werden, sodass sämtliche Bilder und Geräusche in der Umgebung übermittelt werden können,

https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf, S. 4 und https://web.archive.org/web/20200905040710/https://www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf#page=1, S. 2 (jeweils abgerufen am 14. Oktober 2025).

Insbesondere ermöglicht die Software auch ein Abhören eines mit dem infizierten Gerät geführten Telefonats und ein Mitlesen von versendeten Textnachrichten (sog. Quellen-Telekommunikationsüberwachung). Weitere Daten von anderen Apps abzugreifen, wird in dem Angebot als *add-on* dargestellt,

https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf, S. 5 (abgerufen am 14. Oktober 2025).

Die Preise für die Spionagesoftware liegen in Millionenhöhe,

https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf, S. 4 (abgerufen am 14. Oktober 2025).

Das Angebot stellt sich dabei nicht nur als bloßer Verkauf einer Software dar. Vielmehr handelt es sich um ein umfassendes Serviceangebot. Dies ergibt sich bereits daraus, dass in einem Abonnement-Modell zwar die Anzahl der erfolgreichen Infiltrationen, aber nicht der Infiltrationsversuche begrenzt ist. „Candiru Ltd." verpflichtet sich vielmehr zur Vornahme unbegrenzter Infiltrationsversuche,

https://web.archive.org/web/20200905040710/https:/www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf#page=1, S. 2 (abgerufen am 14. Oktober 2025).

Teil des Angebots ist zudem ein „Onboarding" und ein „Operator's und Administrator Training" sowie ein „On Job Training", weitergehende Trainingskurse (Additional Training Advanced Courses) können zusätzlich vereinbart werden,

https://web.archive.org/web/20200905040710/https:/www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf#page=1, S. 3, 5 (abgerufen am 14. Oktober 2025).

Auch sind Wartung, Updates und Gewährleistung der Funktionsfähigkeit Teil des Angebots,

https://web.archive.org/web/20200905040710/https:/www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf#page=1, S. 3 f. (abgerufen am 14. Oktober 2025).

Es ist zwar nicht nachgewiesen, wie viel Kenntnis und Einblick Mitarbeiter*innen der „Candiru Ltd." in die tatsächliche Nutzung ihrer Softwares und Services haben. Für weitgehende Einblicke sprechen jedoch die umfassenden Serviceangebote. Auch zum Schutz von Unternehmensgeheimnissen wie genutzten Sicherheitslücken haben Unternehmen wie die „Candiru Ltd." ein Interesse daran, dass Kund*innen möglichst geringen Zugang zu den Softwareprodukten haben. Ebenso dafür sprechen Äußerungen von Mitarbeiter*innen anderer Unternehmen mit Spionagesoftwareservices, die bestätigen, dass bei den Unternehmen Kenntnis von den konkreten Angriffen und ihren Zielen besteht:

> „The U.A.E. did not respond to multiple requests for comment, and NSO employees told me that the company was unaware of the hack. One of them said, "We hear about every, every phone call that is being hacked over the globe, we get a report immediately"—a statement that contradicts the company's frequent arguments that it has little insight into its customers' activities."

https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens (abgerufen am 14. Oktober 2025).

Im Falle der NSO-Group und der von ihr angebotenen Spionagesoftware „Pegasus" konnten Kund*innen u.a. ein „monitoring system" und einen „24/7 support", aber auch weitgehende „Support Levels" mit Mitarbeiter*innen des Anbieters hinzubuchen, die vor Ort bei der Nutzung der Software unterstützten,

> Attachment 1 zur Beschwerde von Facebook Inc., WhatsApp Inc. gegen die NSO Group Technologies Limited, Q Cyber Technologies Limited vom 29. Oktober 2019, S. 103, 108 (Exhibit 11, S. 37, 43), abrufbar unter https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.1.1_7.pdf (abgerufen am 14. Oktober 2025).

Berichten zufolge werden mit Spionagesoftware von „Candiru Ltd." u.a. Politiker*innen, Menschenrechtsaktivist*innen, Journalist*innen, Akademiker*innen, Botschaftsangehörige und politisch Andersdenkende angegriffen,

> https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#exploit-techniques; https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list (jeweils abgerufen am 14. Oktober 2025).

IV. Zu Einsätzen von Spähsoftware durch Ungarn

Wie bereits dargestellt, werden Systeme von „Candiru Ltd." auch vom ungarischen Staat genutzt,

> https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/, S. 7 (abgerufen am 14. Oktober 2025).

Dabei hat Ungarn bereits in der Vergangenheit Spähsoftware anderer Anbieter*innen rechtsstaatswidrig für Spionage eingesetzt. Dies gilt insbesondere für die Software „Pegasus“ der NSO-Group,

> https://www.amnesty.at/news-events/news/pegasus-projekt-in-zusammenarbeit-mit-amnesty-aktivist-innen-journalist-innen-und-politiker-innen-weltweit-mit-nso-spyware-ausgespaeht/ (abgerufen am 14. Oktober 2025), dazu ausführlich Europäisches Parlament, Bericht über die Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (Bericht A9-0189/2023), Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware, Berichterstatterin: Sophie in ‘t Veld, Rn. 81 ff. (im Folgenden Europäisches Parlament, Bericht A9-0189/2023, Rn.).

Betroffen waren in Ungarn fast 300 Personen,

> https://www.euractiv.com/short_news/hungary-employed-pegasus-spyware-in-hundreds-of-cases-says-government-agency/ (abgerufen am 14. Oktober 2025).

Unter den angegriffenen Personen in Ungarn waren Journalist*innen, aber auch Unternehmer*innen und lokale Politiker*innen,

> https://www.euractiv.com/short_news/hungary-employed-pegasus-spyware-in-hundreds-of-cases-says-government-agency/; https://www.nzz.ch/international/pegasus-in-ungarn-ausspionierte-orban-kritiker-kein-dementi-ld.1636774 (jeweils abgerufen am 14. Oktober 2025) sowie im Einzelnen Europäisches Parlament, Bericht A9-0189/2023, Rn. 110, 111 ff., 115 ff., 120 ff., 123, 124, 125 f., 127 ff.

Daneben ist Ungarn auch Kunde bei zahlreichen weiteren Spähsoftware-Firmen wie Black Cube und Cytrox, die insbesondere im Kontext von Wahlen in Ungarn an Ausspähversuchen beteiligt waren,

> Europäisches Parlament, Bericht A9-0189/2023, Rn. 129 ff.

In Ungarn ist der staatliche Einsatz von Spähsoftware nur unzureichend gesetzlich eingeschränkt, insbesondere, weil für Überwachungen im Kontext von Terrorismus keine richterliche Genehmigung erforderlich ist, sondern eine Genehmigung durch den*die Justizminister*in erfolgt, wobei diese Entscheidungen zum Teil delegiert werden,

> Europäisches Parlament, Bericht A9-0189/2023, Rn. 87 ff., 91 ff.

Eine ausreichende Kontrolle im Vorfeld (ex-ante) ist dabei ebenso wenig sichergestellt wie wirksame Kontrollmechanismen im Nachgang (ex-post),

> Europäisches Parlament, Bericht A9-0189/2023, Rn. 90 ff., 96 ff.

Auch effektiver Rechtsschutz und wirksame Rechtsbehelfe sind nicht gewährleistet,

> Europäisches Parlament, Bericht A9-0189/2023, Rn. 101 ff.

Der Einsatz von Überwachungsmaßnahmen ist vielmehr vollständig politisch kontrolliert,

Europäisches Parlament, Bericht A9-0189/2023, Rn. 106 ff.

Dass die rechtlichen Rahmenbedingungen in Ungarn zu Überwachungsmaßnahmen menschenrechtswidrig sind, wurde auch bereits durch den Europäischen Gerichtshof für Menschenrechte (EGMR) festgestellt,

EGMR, Urteil vom 12. Januar 2016 – 37138/14, Szabó and Vissy v. Hungary, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]} (abgerufen am 14. Oktober 2025).

Ungarn hat jedoch weder dieses Urteil noch weitere Vorgaben des EGMR umgesetzt,

Europäisches Parlament, Bericht A9-0189/2023, Rn. 89.

Es ist davon auszugehen, dass auch die rechtlichen Rahmenbedingungen für Überwachungsmaßnahmen im Ausland, durch den Auslandsgeheimdienst Információs Hivatal (Intelligence Office) menschenrechtlichen und europarechtlichen Anforderungen nicht genügen.

Im Bericht des Untersuchungsausschusses zum Einsatz von Pegasus wird die Situation in Ungarn zur Nutzung von Spähsoftware wie folgt zusammengefasst:

> „Der Einsatz von Pegasus in Ungarn scheint Teil einer kalkulierten und strategischen Kampagne zur Zerstörung der Medienfreiheit und Meinungsfreiheit durch die Regierung zu sein […]. Die Regierung hat diese Spähsoftware genutzt, um leicht und ohne Angst vor Regressansprüchen ein Regime der Belästigung, Erpressung, Drohungen und Druckausübung gegen unabhängige Journalisten, Medien, politische Gegner und Organisationen der Zivilgesellschaft aufzubauen. […]
>
> Das Gesetz, das das Abfangen von Informationen erlaubt, ist viel mehr ein Instrument der Kontrolle und Ausübung von Macht für die Regierung als ein Schutzschild für die Rechte und die Privatsphäre der Bürger und ist zudem eines der schwächsten Gesetze in Europa […]. Das System besteht im Rahmen einer offenkundigen Verletzung der europäischen Anforderungen und Standards in Bezug auf die Überwachung der Bürger in der Europäischen Menschenrechtskonvention und gegen die Urteile des EGMR […]. Obwohl die Regierung immer wieder auf Gründe der „nationalen Sicherheit“ verweist […], sind ihre Behauptungen, dass die Zielpersonen eine Bedrohung der nationalen Sicherheit darstellen, nicht glaubwürdig.“

Europäisches Parlament, Bericht A9-0189/2023, Rn. 132, 133.

Im Zuge dessen kam das Europäische Parlament 2023 zu dem Schluss, dass es in Ungarn zu erheblichen Verstößen und Missständen bei der Umsetzung von Unionsrecht gekommen ist und forderte Ungarn zu konkreten Maßnahmen, gerade auch mit Blick auf die Verwendung von und den Schutz vor Spähsoftware, auf,

> Europäisches Parlament, Prüfung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware (Empfehlung), Empfehlung des Europäischen Parlaments vom 15. Juni 2023 an den Rat und die Kommission nach der Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und

Spähsoftware (2023/2500(RSP), S. 16, Ziff. 17, 18 und https://www.europarl.europa.eu/news/de/press-room/20230609IPR96217/spahsoftware-parlament-fordert-umfassende-untersuchungen-und-schutzvorkehrungen (abgerufen am 14. Oktober 2025).

V. Die versuchte Installation der Spionagesoftware

Der Anzeigenerstatter Daniel Freund war am […] zwischen […] für Wahlkampfveranstaltungen unterwegs. Er hielt sich gerade am […] auf, als er um 14:21:36 Uhr eine E-Mail von der vermeintlichen Absenderin „[…]“ bzw. „[…]“ ([…]) an sein parlamentarisches E-Mail-Postfach […] erhielt. Er führte dabei sein Mobiltelefon und sein Laptop mit sich, auf dem ihm die E-Mail zugestellt wurde.

[…]

Die E-Mail stammte angeblich von einer Studentin der […] University, die an einem Seminar zu Beitrittsmöglichkeiten der Ukraine zur EU teilnahm. Dafür wurde von dem Abgeordneten eine kurze Nachricht erbeten, die die vorgebliche Absenderin mit weiteren Studierenden teilen wollte. Weiterhin enthielt die E-Mail einen Link zu einer vermeintlichen Webseite über das Studierendenparlament, bei dessen Anklicken das Handy des Anzeigeerstatters zu 1) mit einem Spähprogramm infiziert worden wäre.

Der Anzeigenerstatter zu 1) klickte allerdings nicht auf den Link, sodass die Infiltration abgewendet werden konnte.

Laut Medienberichterstattung gab es an der […] University eine Studierende namens […]. Diese betonte auf Medienanfrage, sie wisse nicht, wer der Anzeigeerstatter zu 1) sei, sie habe die E-Mail nicht gesendet und kenne auch das Google-Mail-Konto nicht, von dem die Nachricht stamme,

> https://www.heise.de/news/Candiru-Neuer-Spyware-Angriff-auf-EU-Abgeordneten-9813814.html (abgerufen am 14. Oktober 2025).

Im Nachgang wurde der Anzeigeerstatter zu 1) durch die Verwaltung des Europäischen Parlaments darauf hingewiesen, dass es sich bei dem Link um einen Angriff mit einer Spähsoftware handelte,

> https://www.politico.eu/article/spyware-target-eu-mep-criticize-hungary-daniel-freund/ (abgerufen am 14. Oktober 2025).

Die E-Mail wurde dort von Cyber-Sicherheitsexpert*innen analysiert, die zu dem Ergebnis kamen, dass in dem Angriff höchstwahrscheinlich die Software des Unternehmens „Candiru Ltd.“ zum Einsatz gekommen war und dass nur der Anzeigeerstatter zu 1) von diesen Absender*innen eine E-Mail erhalten hatte

> „[…] **Which spyware was used for the attack?** Based on Threat Intelligence sources made available to the European Parliament, we believe with a medium-high level of confidence that the spyware used for the attack was Candiru. As you know this deduction is based on the email you received from the address “[…]”; this is the only element on which the deduction is made and is not a very specific one.

If indeed Mr. Freund was the only MEP targeted this time; It is possible to confirm that the email from the mentioned sender was sent only to MEP Freund within a reasonable period."

Mail […], Anlage 1).

C. Rechtliche Würdigung

Es besteht der Verdacht, dass sich Unbekannte durch den Angriff mittels Spähprogrammen des Unternehmens „Candiru Ltd." gegen den Anzeigenerstatter zu 1) insbesondere gemäß § 201 Abs. 1 Nr. 1, Abs. 2 Nr. 1, Abs. 4 i.V.m. §§ 22, 23 Abs. 1, § 202c Abs. 1 Nr. 2 StGB sowie gemäß § 303a Abs. 1, 2, 3 und § 303b Abs. 1, 3, 5 StGB strafbar gemacht haben (I.).

Hinzu kommen tatsächliche Anhaltspunkte für eine Strafbarkeit unbekannter Mitarbeiter*innen der „Candiru Ltd." (dazu unter II.) sowie ungarischer Regierungsverantwortlicher, insbesondere des Ministerpräsidenten Viktor Orbán (dazu unter III.).

I. Anfangsverdacht gegen die unbekannten Personen durch das Erstellen und Zuleiten der manipulierten E-Mail sowie durch Erwerb bzw. Beschaffung der Spionagesoftware

1. §§ 201 Abs. 2 Satz 1 Nr. 1, Abs. 4 i.V.m. §§ 22, 23 Abs. 1 StGB

Die Ersteller*innen und Versender*innen der E-Mail haben sich mit hoher Wahrscheinlichkeit wegen versuchter Verletzung der Vertraulichkeit des Wortes nach §§ 201 Abs. 2 Satz 1 Nr. 1 Abs. 4, 22, 23 Abs. 1 StGB strafbar gemacht. Mangels Installation der Software und damit mangels unbefugten Abhörens kam es nicht zu einem Erfolgseintritt.

a) Anwendbarkeit deutschen Strafrechts

Deutsches Strafrecht ist gemäß § 3 StGB i.V.m. § 9 Abs. 1 Var. 4 StGB anwendbar. Da mangels Eintritts des tatbestandlichen Erfolges ein strafbarer Versuch vorliegt, ist für die Anwendbarkeit deutschen Strafrechts die Tatbegehung und damit der Ort maßgeblich, wo nach der Vorstellung der Täter*innen der tatbestandliche Erfolg eintreten sollte.

Da sich der Anzeigeerstatter zu 1) zur Zeit des Angriffs mit seinem Laptop und seinem Mobiltelefon in Deutschland, genauer in Aachen, befand, wäre der tatbestandliche Erfolg des Abhörens nach der Vorstellung der unbekannten Täter*innen auch in Aachen eingetreten, sodass deutsches Strafrecht nach §§ 3, 9 Abs. 1 Var. 4 StGB Anwendung findet.

b) Tatbestandsmäßigkeit

aa) Tatentschluss

Die bislang unbekannten Ersteller*innen und Versender*innen der E-Mail hatten einen Tatentschluss hinsichtlich der Verwirklichung des objektiven Tatbestands, mithin Vorsatz bezüglich des unbefugten Abhörens des nicht-öffentlich gesprochenen Wortes mit einem Abhörgerät.

aaa) Abhören mit Abhörgerät

Die Täter*innen wollten insbesondere das mit einer Spionagesoftware infiltrierte Gerät des Anzeigeerstatters zu 1) und damit ein Abhörgerät gebrauchen, um Gespräche des Anzeigeerstatters zu 1) abzuhören.

Abhörgeräte sind technische Vorrichtungen jeglicher Art, die das gesprochene Wort über dessen normalen Klangbereich hinaus durch Verstärkung oder Übertragung unmittelbar wahrnehmbar machen (BeckOK StGB/*Heuchemer*, 66. Ed. 1.8.2025, StGB § 201 Rn. 11; TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 201 Rn. 19). Durch die ohne Wissen des Anzeigeerstatters zu 1) installierte Software wollten die Täter*innen unbemerkt sowohl Telefongespräche als auch persönliche Gespräche des Anzeigeerstatters zu 1) mithören und aufzeichnen. Durch die Spionagesoftware sollte das Mobiltelefon oder der Computer des Anzeigeerstatters zu 1) daher zu einem Abhörgerät im Sinne des § 201 Abs. 2 Satz 1 Nr. 1 StGB werden, da durch diese das gesprochene Wort über den erwarteten Klangbereich hinaus übertragen und wahrnehmbar gemacht werden sollte.

Eine andere Bewertung ergibt sich auch nicht daraus, dass nach einer älteren Rechtsprechung des Bundesgerichtshofs im Telefon eingebaute Lautsprecher, Zweithörer oder sonstige Mithöreinrichtungen nicht als Abhörgeräte im Sinne des § 201 Abs. 2 Satz 1 Nr. 1 StGB anzusehen sein sollen (BGH, Urteil vom 17. Februar 1982 – VIII ZR 29/81, juris Rn. 19; BGH, Urteil vom 8. Oktober 1993 – 2 StR 400/93, juris Rn. 23, 25, 27). Der BGH begründete seine Entscheidung maßgeblich mit der einschränkenden Auslegung des weit gefassten Tatbestands von § 201 StGB (BGH, Urteil vom 17. Februar 1982 – VIII ZR 29/81, juris Rn. 19; BT-Drucks. 7/550, S. 236).

Diese Rechtsprechung ist nicht mehr zeitgemäß. Sie wird zutreffend als zu eng kritisiert, da es nicht pauschal auf das Gerät, sondern auf die konkrete Art der Nutzung ankommen muss (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 201 Rn. 19 m.w.N.; *Fischer*, StGB, 72. Aufl. 2025, § 201 Rn. 7a). Die Rechtsprechung berücksichtigt die durch technischen Fortschritt entstandenen Nutzungsmöglichkeiten eines Mobiltelefons nicht ausreichend. Ebenso wenig finden Manipulations- und Infiltrationsmöglichkeiten für heute stets mitgeführte Smartphones Berücksichtigung. Aufgrund dieser technischen Entwicklungen bedarf es keiner physischen Abhörvorrichtung mehr. Mittels Software kann nun auf die betroffenen Geräte direkt ohne physische Mithörvorrichtungen Einfluss genommen werden. Eine sinnvolle gerätebezogene Unterscheidung zwischen Telefon und Abhörgerät lässt sich daher, gerade bei Smartphones, nicht mehr treffen (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 201 Rn. 19 m.w.N.). Dies gilt umso mehr, da heute eine vergleichbare Kommunikation auch auf anderen Geräten wie Computern und Tablets möglich ist. Ein Computer kann zwar auch zur Fernkommunikation mittels SIM-Karte oder eSIM genutzt werden, er ist in seiner Funktion von einem Telefon gleichwohl zu unterscheiden, da er schwerpunktmäßig nicht der telefonischen Kommunikation dient. Jedenfalls Computer und Tablets können nicht pauschal aus dem Tatbestand des § 201 Abs. 2 StGB ausgenommen sein.

Vielmehr kann es nur auf die jeweilige Funktion bzw. Bedienweise des Gerätes beim konkreten Einsatz ankommen (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 201 Rn. 19 m.w.N.). Nur durch eine solche Unterscheidung kann der konkreten technischen Ausgestaltung Rechnung getragen werden und das Rechtsgut des Betroffenen, der Schutz vor „technischer Ausdehnung des Klangbereichs“ und damit vor dem Ausspähen der Persönlichkeitssphäre ausreichend geschützt werden. In Fällen, in welchen ein (Mobil-)Telefon oder anderes Fernsprechgerät ohne

Wissen der Kommunikationsteilnehmer von einem Dritten mit einer Spionagesoftware infiltriert wird und die Kommunikation während des Übermittlungsvorgangs abgehört wird, ist in diesem Gerät daher ein Abhörgerät im Sinne der Norm zu sehen.

Selbst unter Anwendung der Grundsätze des BGHs ist vorliegend jedoch nach Vorstellung der Täter*innen ein Abhörgerät gegeben.

Die Rechtsprechung beschränkt die Ausnahme von Telefonen aus dem Tatbestand insoweit auf „übliche und von der Post zugelassene Mithöreinrichtungen“, bei denen regelmäßig mit der Einbeziehung eines Mithörers zu rechnen ist (BGH, Urteil vom 8. Oktober 1993 – 2 StR 400/93, juris Rn. 23, 25, 27 mit Verweis auf BGH, Urteil vom 17. Februar 1982 – VIII ZR 29/81, juris Rn. 19). Dies gilt mithin für Fälle, in denen ein (Mobil-)Telefon bestimmungsgemäß zur Kommunikationsübermittlung durch angewählte oder angenommene Telefonate genutzt wird und am Ende dieser Übermittlung ein Mithören durch eine zulässige Mithöreinrichtung ermöglicht wird. Dies ist im konkreten Fall aber nicht gegeben.

Vorliegend handelt es sich um eine heimliche Infiltration des Geräts, die es auch ermöglicht, dass Gespräche in der Nähe des Mobiltelefons abgehört werden. So können durch Zugriff auf das Mikrofon des infiltrierten Geräts auch solche Gespräche abgehört werden, die nicht mittels Fernsprecher geführt werden. Bereits der zugrundeliegende Hergang ist daher nicht vergleichbar.

Aber auch bei mitgehörten Telefonaten über das infiltrierte Gerät handelt es sich nicht um übliche und zugelassene Mithöreinrichtungen, da nicht auf der Seite der Kommunikationsempfänger*innen, sondern direkt im Gerät des Infiltrierten heimlich mitgehört wird. Die Mithörer*innen stehen somit, anders als beim bloßen Mithören über Lautsprecher oder Zweithörer, nicht auf der Seite und im Einverständnis eines*einer Gesprächsteilnehmer*in und am Ende der Kommunikation, sondern infiltriert den von Art. 10 GG geschützten Übermittlungsvorgang selbst. Zudem ist die Möglichkeit einer – wie oben skizzierten – Zweckentfremdung des geräteeigenen Mikrofons nur mit aufwendigen, hochpreisigen Spähprogrammen gegeben und dementsprechend selten. Durch diese Software ist es möglich, bei Telefonaten oder vertraulichen Gesprächen durch das eigene Handy abgehört zu werden. Es handelt sich keinesfalls um eine übliche zulässige Mithöreinrichtung, mit der der Anzeigeerstatter zu 1) hätte rechnen müssen. Zuletzt sei darauf hingewiesen, dass der Link dem Anzeigeerstatter zu 1) per E-Mail zugesendet worden ist. Damit war der Vorsatz der Täter*innen nicht darauf beschränkt, dass das Mobiltelefon des Anzeigeerstatters zu 1) infiltriert werde würde, da dieser seine Mails auf mehreren Computern und seinem Mobiltelefon empfängt.

Auch war der Vorsatz der Täter*innen darauf gerichtet, das infizierte Smartphone als Abhörgerät zum Abhören zu benutzen. Ein Abhören liegt bei einer gezielten Nutzung des Abhörgeräts vor. Da die Angreifenden dem Anzeigeerstatter zu 1) einen infizierten Link in einer gefälschten E-Mail zusendeten und somit eine heimliche Installation der Software erfolgen sollte, ist davon auszugehen, dass sie das Smartphone nach dem erfolgreichen Angriff auch tatsächlich zum Abhören verwenden wollten. Die Erstellung einer solchen manipulierten E-Mail sowie der Erwerb und Einsatz solcher Spionagetools sind mit Aufwand und Kosten in Millionenhöhe verbunden, sodass es ausgeschlossen erscheint, dass es sich bei der Zusendung der Software um ein Versehen handelt oder die Angreifer*innen davon keinen Gebrauch machen wollten.

bbb) Nichtöffentlich gesprochenes Wort

Der Tatentschluss der unbekannten Täter*innen umfasste auch das Abhören des nicht öffentlich gesprochenen Wortes. Die Täter*innen zielten mit E-Mailversendung gerade darauf ab, dass der Anzeigeerstatter zu 1) die Spionagesoftware auf seinem Gerät installieren würde, ohne es zu bemerken und sein Telefon sodann unwissend über die Zugriffsmöglichkeiten weiter nutzen würde. Die Software sollte damit gerade den Zugriff auch auf Telefonate und nichtöffentliche Gespräche zwischen Personen ermöglichen, die im Privaten und abgegrenzt geführt werden und deren Inhalte anderen Personen nicht zugänglich sein sollten.

Es war mithin gerade das bewusste Ziel der Täter*innen, Gespräche abzuhören, die nichtöffentlich und daher auch nicht zu ihrer Kenntnis bestimmt waren.

bb) Unmittelbares Ansetzen, § 22 StGB

Mit dem Zusenden der E-Mail an den Anzeigeerstatter zu 1) haben die Täter*innen auch unmittelbar angesetzt, § 22 StGB.

Nach dem herrschenden Kombinationsansatz müssen die Täter*innen subjektiv die Schwelle zum „Jetzt-geht-es-los“ überschreiten und objektiv zur tatbestandsmäßigen Handlung ansetzen, sodass das Tun ohne wesentliche Zwischenakte in die Tatbestandserfüllung übergeht (BGH, Beschluss vom 29. April 2014 – 3 StR 21/14, juris Rn. 6 m.w.N.; BGH, Urteil vom 16. September 1975 – 1 StR 264/75, juris Rn. 19; BeckOK StGB/*Cornelius*, 66. Ed. 1.5.2025, StGB § 22 Rn. 35; TK-StGB/*Bosch*, 31. Aufl. 2025, StGB § 22 Rn. 41).

Bei Distanz- oder Fernwirkungsfällen liegt ein unmittelbares Ansetzen vor, wenn die Täter*innen das von ihnen in Gang gesetzte Geschehen in der Weise aus der Hand gegeben haben, dass der daraus resultierende Angriff auf das Opfer nach ihrer Vorstellung von der Tat ohne weitere wesentliche Zwischenschritte und ohne längere Unterbrechung im nachfolgenden Geschehensablauf unmittelbar in die Tatbestandsverwirklichung einmünden soll (BGH, Urteil vom 26. Januar 1982 – 4 StR 631/81, juris Rn. 5).

Konkret für den Fall des § 201 StGB beginnt nach Ansicht der Literatur ein Versuch in allen Tatvarianten dann, wenn der Täter sich anschickt, das Abhörgerät einzuschalten (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 201 Rn. 36).

Dies ist hier der Fall. Der vorliegende Geschehensablauf gleicht unter den ausschlaggebenden Gesichtspunkten dem Einschalten eines Abhörgeräts:

Mit dem Absenden der manipulierten E-Mail haben die Täter*innen das Geschehen vollständig aus der Hand gegeben und die aus ihrer Sicht vorzunehmende Handlung zur Verwirklichung des objektiven Tatbestandes vorgenommen, da es zur Installation ausschließlich des Anklickens des Links durch den Anzeigeerstatter zu 1) bedarf. Bei einem Klick handelt es sich dabei um eine täglich tausendfach vorgenommene niedrigschwellige Mitwirkung, die auch versehentlich oder unbewusst erfolgen kann. So mündet die Verwendung der E-Mail mit der Software unmittelbar in die Tatbestandsverwirklichung – nämlich der Abhörung des Anzeigeerstatters zu 1) durch dessen Gerät. Es ist dabei davon auszugehen, dass die Software von „Candiru Ltd.“ mit Abschluss der vollautomatisch ablaufenden Installation sofort aktiviert ist und damit sofort ohne weitere Zwischenschritte mithört und Inhalte übermittelt. Die Installation erfolgt vollautomatisiert und ist für die Betroffenen auch nicht erkennbar. Es bedarf daher aus Sicht der Täter*innen auch keiner weiteren eigenen Tathandlungen. Mit dem Abschluss der

vollautomatisierten Installation der Software sollte nach ihrer Vorstellung das Gerät unmittelbar wie ein bereits angeschaltetes Abhörgerät eingesetzt werden.

Daher kommt es auf eine etwaige Aktivierung der Software durch die Täter*innen auch nicht an. Eine solche ist nach Abschluss der Installation aus ihrer Sicht bereits erfolgt.

Selbst wenn die unbekannten Täter*innen nach Benachrichtigung über die erfolgreiche Installation der Software das Gerät als Abhörgerät noch aktivieren müssten, stellt dieses Aktivieren bzw. Anschalten einen nur unwesentlichen Schritt dar.

So genügt es, dass sich Täter*innen anschicken, das Tonbandgerät einzuschalten (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 201 Rn. 36). Mit Abschluss des automatisierten Herunterladens ist das Gerät sofort bereit, den Angreifer*innen über ein Mitlaufen des Mikrofons vertrauliche Gesprächsinhalte zu übermitteln und kann ohne weiteres zum Abhören in Betrieb genommen werden. Ein erforderliches Anschicken ist anzunehmen, da das Gerät aller Wahrscheinlichkeit nach sofort nach Abschluss der Installation aktiviert wird. Anhaltspunkte dafür, dass die Täter*innen nach dem Aufwand für die erfolgreiche Infiltration mit dem Ziel des Abhörens mit der Aktivierung des geräteeigenen Mikrofons zögern würden, liegen nicht vor und sind bei einer lebensnahen Betrachtung des Sachverhalts auch fernliegend.

c) Strafantrag

Gemäß § 205 Abs. 1 Satz 1 StGB handelt es sich bei § 201 StGB um ein absolutes Antragsdelikt. Der Strafantrag gegen unbekannt wird hiermit auch vom Verletzten Daniel Freund als Anzeigeerstatter zu 1) gestellt.

Die Antragsfrist des § 77b Abs. 1 StGB hat nicht zu laufen begonnen, da der Verletzte noch keine Kenntnis von der Person der Täter*innen hat, § 77b Abs. 2 StGB (TK-StGB/*Bosch*, 31. Aufl. 2025, StGB § 77b Rn. 9).

2. §§ 201 Abs. 1 Nr. 1, Abs. 4 i.V.m. §§ 22, 23 Abs. 1 StGB

Mit hoher Wahrscheinlichkeit kommt eine Strafbarkeit der Unbekannten ferner wegen versuchter Verletzung der Vertraulichkeit des Wortes nach §§ 201 Abs. 1 Nr. 1, Abs. 4, 22, 23 Abs. 1 StGB in Betracht, insoweit besteht ein Anfangsverdacht. Der Versuch ist in allen Fällen des § 201 StGB strafbar (§ 201 Abs. 4 i.V.m. 23 Abs. 1 StGB).

a) Anwendbarkeit deutschen Strafrechts

Deutsches Strafrecht ist gemäß §§ 3, 9 Abs. 1 StGB anwendbar (s. dazu bereits 1. a)).

b) Tatbestandsmäßigkeit

aa) Tatentschluss

Die unbekannten Täter*innen hatten auch Tatentschluss, also den Vorsatz, sämtliche objektiven Tatbestandsmerkmale des § 201 Abs. 1 Nr. 1 StGB zu verwirklichen. Für den Fall des § 201 Abs. 1 Nr. 1 StGB erfordert dies Vorsatz hinsichtlich einer unbefugten Aufnahme des nichtöffentlich gesprochenen Wortes auf einen Tonträger.

Der Tatentschluss der Täter*innen richtete sich auf eine Verletzung des nichtöffentlich gesprochenen Wortes des Anzeigenerstatters zu 1) (siehe dazu bereits oben 1.b) aa) bbb)).

Zusätzlich erfordert diese Tatbestandsvariante des § 201 Abs. 1 Nr. 1 StGB lediglich das Aufnehmen des gesprochenen Wortes auf einen Tonträger. Auch diesbezüglich war ein Tatentschluss gegeben.

Aufnehmen ist das Fixieren des geäußerten Wortes auf technischem Wege auf einen beliebigen Tonträger in der Weise, dass eine (wiederholte) akustische Reproduktion und Wahrnehmung hierdurch möglich ist (BeckOK StGB/*Heuchemer*, 66. Ed. 1.8.2025, StGB § 201 Rn. 5; TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 201 Rn. 11). Tonträger ist dabei jede Vorrichtung zur wiederholten Wiedergabe von Tonfolgen (Lackner/Kühl/Heger, 31. Aufl. 2025, StGB § 201 Rn. 3; vgl. auch BGH, Urteil vom 24. November 1981 – VI ZR 164/79, juris Rn. 8, der von einer „Tonkonserve“ spricht).

Die Spähsoftware von „Candiru Ltd.“ ermöglicht es auch, die Hardware des infiltrierten Geräts für Aufnahmen zu nutzen. Ohne Speicherung des abgehörten, nichtöffentlich gesprochenen Wortes des Anzeigeerstatters zu 1) würde das ein ggf. zeitzonenübergreifendes, zeitgleiches Abhören vonseiten der Täter*innen erfordern und eine nur sehr eingeschränkte Verwertbarkeit des abgehörten Materials durch den jeweils akustisch direkt vernehmenden Täter*innen bedeuten. Vor dem Hintergrund dieser Erwägungen und angesichts des strategisch geplanten, professionellen Vorgehens zielte das Handeln der Täter*innen mit hoher Wahrscheinlichkeit auch auf das Anfertigen von Aufnahmen ab. Folglich ist auch das Aufnehmen auf einem Tonträger vom Vorsatz der Täter*innen umfasst.

bb) Unmittelbares Ansetzen, § 22 StGB

Mit der Zusendung des manipulierten Links haben die Täter*innen auch zur Verwirklichung von § 201 Abs. 2 StGB unmittelbar angesetzt. Ab der Installation der Software ist in nächster Zukunft und ohne wesentliche Zwischenschritte mit einer Aktivierung der Software auch als Aufnahmegerät zu rechnen. Abhören und Aufnehmen fallen nach Vorstellung der Täter*innen zeit- und deckungsgleich zusammen.

c) Strafantrag

Der Strafantrag des Anzeigeerstatters zu 1) und Verletzten soll auch die Tatbestandsvariante des § 201 Abs. 1 Nr. 1 StGB umfassen.

3. § 202c Abs. 1 Nr. 2 Var. 2 StGB

Die unbekannten Täter*innen haben sich zudem mit hoher Wahrscheinlichkeit gemäß § 202c Abs. 1 Nr. 2 Var. 2 StGB strafbar gemacht, auch diesbezüglich besteht ein Anfangsverdacht. Fraglich ist insoweit lediglich die Anwendbarkeit des deutschen Strafrechts.

a) Anwendbarkeit deutschen Strafrechts

Da es sich bei § 202c StGB um ein abstraktes Gefährdungsdelikt handelt (BeckOK StGB/*Weidemann*, 66 Ed. 01.08.2025, StGB § 202c Rn. 3 m.w.N.), käme deutsches Strafrecht insbesondere zur Anwendung, wenn die Täter*innen die Tathandlungen in Deutschland vorgenommen haben, §§ 3, 9 Abs. 1 Var. 1 StGB, oder in den Fällen des § 7 Abs. 2 StGB. Dies ist jedenfalls nicht ausgeschlossen und mit der Person der Täter*innen zu ermitteln.

Insbesondere ist die begangene Tat gemäß § 7 Abs. 2 StGB auch im wahrscheinlichen Begehungsland Ungarn mit Strafe bedroht. Die Regelung des § 424 Abs. 1 lit. a des ungarischen

Strafgesetzbuchs in der am 1. Juli geltenden Fassung entspricht im Wesentlichen dem § 202c Abs. 1 Nr. 2 StGB. Beide Vorschriften dienen der Umsetzung der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates. Unter Strafe gestellt ist ebenso das Zugänglichmachen eines Computerprogramms, das für die Begehung einer Straftat erforderlich ist oder diese erleichtert, zum Zwecke einer Straftat (https://njt.hu/jogszabaly/en/2012-100-00-00, S. 149 (abgerufen am 14. Oktober 2025)).

b) Tatbestand

Durch den Ankauf bzw. Erwerb der Spionagesoftware der „Candiru Ltd." haben sich die unbekannten Täter*innen Computerprogramme im Sinne des § 202c Abs. 1 Nr. 2 StGB verschafft.

Computerprogramme im Sinne des § 202c Abs. 1 Nr. 2 Var. 2 StGB umfassen sogenannte Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen und die durch das Internet eine weite Verbreitung erfahren (BT-Drs. 16/3656, 12; BeckOK StGB/*Weidemann*, 66. Ed. 1.8.2025, StGB § 202c Rn. 6). Umfasst sind daher nur Programme, deren (objektivierte) Zweckbestimmung es ist, eine Straftat nach §§ 202a, 202b StGB zu begehen (BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08, juris Rn. 60 f.; BeckOK StGB/*Weidemann*, 66. Ed. 1.8.2025, StGB § 202c Rn. 6; TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 202c Rn. 4). Maßgeblich ist die Absicht des Herstellers, die sich äußerlich im Programm manifestiert haben muss (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 202c Rn. 4). Durch die an § 263a Abs. 3 StGB angelehnte Einschränkung soll sichergestellt werden, dass allgemeine Programmier-Tools, -sprachen oder sonstigen Anwendungsprogramme nicht bereits unter den objektiven Tatbestand der Strafvorschrift fallen (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 202c Rn. 4).

Eine solche Manifestation der Absicht bzw. des Zweckes kann in der Gestalt des Programms selbst liegen, im Sinne einer Verwendungsabsicht, die sich nunmehr der Sache selbst interpretativ ablesen lässt. Diese kann sich aber auch aus einer eindeutig auf illegale Verwendungen abzielenden Vertriebspolitik und Werbung des Herstellers ergeben (BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08, juris Rn. 66).

Bereits die Entstehungsgeschichte der Norm spricht für die Berücksichtigung des Manifestationswillens der Entwickler*innen (BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08, juris Rn. 65). Der Straftatbestand des § 202c Abs. 1 Nr. 2 StGB dient zur Umsetzung von Art. 6 Abs. 1 lit. a Nr. 1 des Übereinkommens des Europarats über Computerkriminalität vom 23. November 2001 (CKÜ) und Art. 7 lit. a RL 2013/40/EU (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 202c Rn. 3). Insbesondere Art. 6 Abs. 1 lit. a Nr. i CKÜ bezieht sich ausdrücklich auf eine „Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen" (BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08, juris Rn. 65), sodass der konkrete Entstehungsvorgang des Programms betrachtet wird.

Dies hat jedoch nicht zur Folge, dass sämtliche Computerprogramme, die auf legale und illegale Weise genutzt werden können, also sog. dual-use-tools generell nicht dem Anwendungsbereich der Norm unterfallen. Nicht umfasst sind nur solche dual-use-tools, die für die Begehung der genannten Computerstraftaten lediglich geeignet oder besonders geeignet sind (BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08, juris Rn. 61; BT-Drs. 16/3656, S. 19). Die bloße Eignung unterscheidet sich deutlich von dem Begriff des Zwecks (BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2

BvR 1524/08, juris Rn. 61). Der Europarat hat jedoch dual-use-devices bewusst nicht aus Art. 6 Abs. 1 lit. a Nr. 1 CKÜ ausgenommen. Danach soll der Begriff der „Computersoftware“ weder zu breit noch zu eng gefasst werden (Explanatory Report – ETS 185 – Cybercrime (Convention) Rn. 73, abrufbar unter https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (abgerufen am 14. Oktober 2025)). Dual-use-tools unterfallen mithin dem Tatbestand des § 202c Abs. 1 Nr. 2 StGB, wenn ihr funktionaler objektiv manifestierter Zweck ausreichend kriminell ist.

Unter Anwendung dieser Grundsätze ist objektivierter Zweck der Spähsoftware der „Candiru Ltd.“ die Begehung einer Tat nach § 202a StGB.

Die Software dient mit hoher Wahrscheinlichkeit dem Zweck, den unbefugten Zugang zu besonders gesicherten Daten im Sinne des § 202a StGB auf den infiltrierten Geräten zu ermöglichen. Diese Zwecksetzung ist auch objektiv manifestiert.

Der objektive Tatbestand des § 202a Abs. 1 StGB erfordert, dass die Täter*innen sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschaffen. Dabei sind Daten nach der Legaldefinition des § 202a Abs. 2 StGB nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Das Eindringen in ein Computersystem durch Zugangsverschaffung setzt weiterhin voraus, dass die Täter*innen den Datenträger in ihre Verfügungsgewalt (oder die eines Dritten) bringen (TK-StGB/*Eisele*, 31. Aufl. 2025, StGB § 202a Rn. 18a).

Der Zweck der Software, nämlich die Verschaffung eines unbefugten Zugangs zu Daten Dritter, ergibt sich bereits aus der in einer geleakten Produktbeschreibung niedergelegten Zwecksetzung der „Candiru Ltd.“ selbst:

> „The system is a high-end cyber intelligence platform dedicated to infiltrate PC computers, networks, mobile handsets by using exploitations and dissemination operations.“ https://web.archive.org/web/20200905040710/https:/www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf#page=1, S. 1 (abgerufen am 14. Oktober 2025).

Das Produkt wurde mithin ausdrücklich gerade dafür hergestellt, Zugang zu besonders gesicherten Daten zu ermöglichen. Dies geht – wie vom Bundesverfassungsgericht gefordert (BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08, juris Rn. 62 f.) – über die bloße Eignung zu einer solchen Nutzung hinaus. Anders als bei sogenannten dual-use-tools wird das Programm daher nicht erst zur Begehung von Straftaten durch die Täter*innen missbraucht, sodass lediglich eine schlichte Eignung des Programms zur Begehung der §§ 202a f. StGB besteht. Vielmehr ist gerade Ziel des Herstellers, eine Schadsoftware zur unerkannten Infiltration von Endgeräten zur Verfügung zu stellen.

Auch aufgrund ihrer objektiven Beschaffenheit und der konkreten Ausgestaltung der zur Verfügung stehenden Computerprogramme verfügt die Software über die erforderliche objektivierte Zweckbestimmung. Die Spionagesoftware ermöglicht nicht nur das Abhören und Aufnehmen von Gesprächen über das infiltrierte Mobiltelefon, sondern auch einen umfassenden heimlichen Zugang zu auf dem Mobiltelefon oder Dienstcomputer gespeicherten Daten aus verschiedenen Apps wie Fotos, Videos, Textnachrichten, Sprachaufnahmen, (auch aus verschlüsselten) Messengerdiensten und Apps (insbesondere Zugriff auf Plattformen der sozialen Medien) und damit auf Daten im Sinne von § 202a StGB. Diese Daten sind durch Passwörter

bzw. Entsperrcodes des Smartphones bzw. Computers sowie durch technische Sicherungsvorkehrungen, die ein unbefugtes Eindringen über Netzwerke verhindern sollen, auch besonders gesichert. Durch den heimlichen Download über einen manipulierten Link verschafft sich die Software den Zugang auch unter Überwindung der Zugangssicherung und damit unter Verletzung von § 202a StGB.

Auch die undurchsichtige Unternehmensstruktur und Arbeitsweise der „Candiru Ltd." legen eine solche Zwecksetzung der Produkte nahe.

Mit hoher Wahrscheinlichkeit ist davon auszugehen, dass die objektive Zwecksetzung der „Candiru Ltd." gerade auch unbefugte und strafbare Infiltrationen durch Staaten von der Zwecksetzung umfasste. Neben den obengenannten Aspekten, insbesondere der Arbeitsweise des Unternehmens spricht hierfür insbesondere die Auswahl der Vertragspartner*innen und die Lizensierung an Staaten wie Saudi-Arabien oder das im konkreten Fall in Verdacht stehende Ungarn. Die Lizensierung an diese Staaten erfolgte trotz bereits bestehender Vorwürfe der rechtsstaatswidrigen Verfolgung und Spionage gegen Journalist*innen und Regierungskritiker*innen. Dies zeigt gerade auch der Angriff auf den Anzeigeerstatter zu 1).

Dass die Software von diesen Staaten möglicherweise auch für die rechtmäßige Überwachung durch Staaten eingesetzt werden kann, schließt eine Zweckbestimmung zur Begehung der genannten Straftaten nicht aus. Anderenfalls wären alle Tools, die insbesondere von Staaten auch rechtskonform genutzt werden könnten, aus dem Anwendungsbereich der Norm ausgenommen, auch wenn diese hochinvasive Eingriffe ermöglichen und eine rechtwidrige Nutzung wahrscheinlich ist. Der Einsatz zu rechtsstaatswidrigen Zwecken war vorliegend mit hoher Wahrscheinlichkeit zumindest zweckprägend. Dies ist im Strafverfahren zu ermitteln.

Die Täter*innen haben sich die Computersoftware auch verschafft, indem sie das Programm angekauft bzw. erworben haben und dadurch die Verfügungsgewalt über diese erhalten haben.

Diesbezüglich handelten die Täter*innen auch vorsätzlich, § 15 StGB.

c) Kein Strafantragserfordernis

Das Strafantragserfordernis des § 205 StGB erstreckt sich nicht auf § 202c StGB.

4. §§ 303a Abs. 1, 2, 22, 23 Abs. 1 StGB bzw. § 303a Abs. 3 i.V.m. § 202c Abs. 1 Nr. 2 StGB und §§ 303b Abs. 1, 2, 3, 22, 23 Abs. 1 StGB bzw. § 303b Abs. 5 i.V.m. § 202c Abs. 1 Nr. 2 StGB

Weiterhin besteht eine hohe Wahrscheinlichkeit, dass sich die unbekannten Täter*innen durch Zusendung des Links gemäß §§ 303a Abs. 1, 2, 22, 23 Abs. 1 bzw. § 303a Abs. 3 i.V.m. § 202c Abs. 1 Nr. 2 StGB und §§ 303b Abs. 1, 2, 3, 22, 23 Abs. 1 StGB bzw. § 303b Abs. 5 i.V.m. § 202c Abs. 1 Nr. 2 StGB strafbar gemacht haben.

a) §§ 303a Abs. 1, 2, 22, 23 Abs. 1 StGB bzw. § 303a Abs. 3 i.V.m. § 202c Abs. 1 Nr. 2 StGB

Die Täter*innen wiesen Tatentschluss hinsichtlich der Verwirklichung des objektiven Tatbestands auf, es kam ihnen gerade darauf an, rechtswidrig Daten (§ 202a Abs. 2 StGB) zu verändern, da es einer solchen Veränderung zur Installation der Spionagesoftware „Candiru" bedurfte.

Schon durch die Installation des Softwareprogramms wäre es zu einer Veränderung von Daten im Sinne des § 202a Abs. 2 StGB gekommen, da dabei Programme bzw. Programmteile und damit Daten (TK-StGB/*Hecker*, 31. Aufl. 2025, StGB § 303a Rn. 2) des infiltrierten Geräts verändert worden wären. Verändert werden Daten, wenn sie einen anderen Informationsgehalt (Aussagewert) erhalten und dadurch der ursprüngliche Verwendungszweck beeinträchtigt wird (TK-StGB/*Hecker*, 31. Aufl. 2025, StGB § 303a Rn. 8). Dazu zählt u.a. das inhaltliche Umgestalten gespeicherter, bzw. Hinzufügen weiterer Daten (BGH, Beschluss vom 27. Juli 2017 – 1 StR 412/16, juris Rn. 33). Entscheidend ist, dass ein vom bisherigen Zustand abweichender Zustand herbeigeführt wird (BGH, Beschluss vom 27. Juli 2017 – 1 StR 412/16, juris Rn. 33).

Vorliegend sollte durch das Anklicken des Links die Schadsoftware unmittelbar, unerkannt und ohne weiteres Zutun auf das Gerät des Anzeigeerstatters zu 1) geladen und dort installiert werden. Durch die Software ist es möglich, auf Daten auf dem Gerät, insbesondere Programme und Programmteilen unerkannt zuzugreifen. In der Produktbeschreibung von „Candiru Ltd." wird diesbezüglich ausgeführt, dass Mitarbeiter*innen Root-Rechte (auch bekannt als Systemrechte) erhalten und dadurch eine unbemerkte Datenexfiltration durch Manipulation und Kontrolle der Gerätehardware und lokaler Programme (z. B. Kommunikationsprogramme, Webcam, Mikrofon usw.) möglich wird,

> https://web.archive.org/web/20200905040710/https:/www.themarker.com/embeds/pdf_upload/2020/20200902-161742.pdf#page=1, S. 1 (abgerufen am 14. Oktober 2025).

Aus Sicht der Täter*innen sollten dabei erhebliche Programmteile unmittelbar nach dem Anklicken des Links durch die heruntergeladene Schadsoftware derart verändert werden, dass unmittelbar Abhör- und Ablesemaßnahmen möglich sind. Diese Daten unterlagen auch nicht der Verfügungsbefugnis der Täter*innen, sodass die Veränderung unbefugt und rechtswidrig erfolgen sollte.

Zu dieser Datenveränderung haben die Täter*innen auch unmittelbar angesetzt, § 22 StGB. Insoweit kann auf die Ausführungen unter C. I. 1. b. bb) verwiesen werden.

Jedenfalls haben sich die Täter*innen mit dem Erwerb der Software der „Candiru Ltd" ein Computerprogramm im Sinne des § 303a Abs. 3 i.V.m. § 202c Abs. 2 Nr. 2 StGB verschafft, insoweit kann auf die Ausführungen unter C. I. 3. verwiesen werden.

b) §§ 303b Abs. 1, 2, 3, 22, 23 Abs. 1 StGB bzw. § 303b Abs. 5 i.V.m. § 202c Abs. 1 Nr. 2 StGB

Es besteht die Wahrscheinlichkeit, dass sich die Täter*innen mit der Installation der Software auch wegen einer versuchten Computersabotage im Sinne der §§ 303b Abs. 1, 2, 3, 22, 23 Abs. 1 StGB bzw. wegen der Vorbereitung einer solchen gemäß § 303b Abs. 5 i.V.m. § 202c Abs. 1 Nr. 2 StGB strafbar gemacht haben.

c) Strafantrag

Auch bezüglich der dargestellten Taten wird der nach § 303c StGB erforderliche Strafantrag gestellt. Jedenfalls besteht aufgrund der hohen Bedeutung des Spähsoftware-Angriffs auf einen Abgeordneten auch ein besonderes öffentliches Interesse an der Strafverfolgung. Durch eine erfolgreiche Infiltration wären die Täter*innen an Informationen aus der Arbeit eines Abgeordneten und damit an sensible Interna der parlamentarischen Arbeit gelangt. Dem Fall

kommt vor diesem Hintergrund besondere, die gesamte Europäische Union betreffende Bedeutung zu.

II. Anfangsverdacht gegen unbekannte Täter*innen wegen Überlassung der Spionagesoftware

Darüber hinaus haben sich mit hoher Wahrscheinlichkeit auch Mitarbeiter*innen des Unternehmens „Candiru Ltd." bzw. der Saito Tech Ltd. der Beihilfe zur versuchten Verletzung der Vertraulichkeit des Wortes nach §§ 201 Abs. 1 Nr. 1, Abs. 1 Nr. 1, Abs. 4, 22, 23 Abs. 1 i.V.m. § 27 StGB strafbar gemacht (1.). Daneben tritt ebenfalls mit hoher Wahrscheinlichkeit eine Strafbarkeit gemäß § 202c Abs. 1 Nr. 2 StGB (2.). Auch insoweit besteht ein Anfangsverdacht.

1. §§ 201 Abs. 1 Nr. 1, Abs. 4 bzw. Abs. 2 Nr. 1, Abs. 4, 22, 23 Abs. 1 i.V.m. § 27 StGB

a) Anwendbarkeit deutschen Strafrechts

Für die Beihilfestrafbarkeiten ist das deutsche Strafrecht anwendbar, §§ 3, 9 Abs. 1, 2 Satz 1 StGB, da die Haupttat im Inland begangen ist (s. dazu oben 1. a) und 2. a)) und damit auch die Teilnahme am Ort der Haupttat und damit in Deutschland begangen ist, § 9 Abs. 2 Satz 1 StGB.

b) Tatbestand der Beihilfestrafbarkeit

Mit dem Infiltrationsversuch und den korrespondieren Strafbarkeiten nach §§ 201 Abs. 1 Nr. 1, Abs. 4 bzw. Abs. 2 Nr. 1, Abs. 4, 22, 23 Abs. 1 StGB ist eine vorsätzliche und rechtswidrige Haupttat gegeben (s. dazu bereits oben).

Hilfeleistung im Sinne des § 27 StGB ist grundsätzlich jede Handlung, welche die Herbeiführung des Taterfolges durch den Haupttäter objektiv fördert oder erleichtert. Dass sie für den Eintritt dieses Erfolges in seinem konkreten Gepräge in irgendeiner Weise kausal wird, ist nicht erforderlich (BGH, Urteil vom 16. November 2006 – 3 StR 139/06, juris Rn. 40).

Die Mitarbeiter*innen stellten die Spähprogramme bereit und erbrachten die damit einhergehenden Dienstleistungen, die mit hoher Wahrscheinlichkeit das Bereitstellen von manipulierten Infiltrationslinks zu gefälschten Webseiten, die Wartung und das Updaten der Systeme sowie die Unterstützung bei technischen Problemen umfassten. Vorliegend ist davon auszugehen, dass die Mitarbeiter*innen den Link zu der vermeintlichen Teamseite der Organisation der angeblichen Absenderin erstellten. Unzweifelhaft ermöglichten diese Handlungen erst den Infiltrationsversuch in seiner konkreten Gestalt durch die unbekannten Haupttäter*innen förderten damit die Haupttat objektiv.

c) Subjektiver Tatbestand

aa) Gehilf*innenvorsatz

Die Mitarbeiter*innen stellten die Software und ihre Dienstleistungen an Vertragspartner*innen zur Verfügung und nahmen dabei mit hoher Wahrscheinlichkeit die Verletzung der Vertraulichkeit des Wortes als Haupttat billigend in Kauf. Der Gehilfenvorsatz bezog sich daher höchstwahrscheinlich sowohl auf das Aufnehmen des nichtöffentlich gesprochenen Wortes als auch

auf das Abhören mit einem Abhörgerät, da beide Angriffe mit den überlassenen Spähprogramme ermöglicht werden.

Der Vorsatz ergibt sich mit hoher Wahrscheinlichkeit bereits aus konkreten Kenntnissen der Mitarbeiter*innen über Ziele der Infiltration. Es sprechen eine Vielzahl von Tatsachen dafür, dass die Mitarbeiter*innen der „Candiru Ltd." nachvollziehen konnten bzw. können, welche Ziele angegriffen werden und wie die Kund*innen die Software gebrauchen. Dafür sprechen zunächst die zugesicherten unbegrenzten Infiltrationsversuche. Nach gescheiterten Angriffsversuchen ist für neue Ansätze erforderlich, dass das Unternehmen möglichst viele Informationen über die Ziele des Angriffs, deren technische Ausstattung und mögliche funktionierende Angriffstechniken und Szenarien erhält. Daneben erfordern auch die zugesicherte Wartungs- und Updateservices, z.B. durch telefonische Unterstützung via Hotline, dass die Mitarbeiter*innen Kenntnis über die Aktivitäten der Kund*innen und Zugriff auf deren Aktivitäten haben, um in kurzer Zeit Probleme beheben zu können. Es ist darüber hinaus unwahrscheinlich, dass „Candiru Ltd." seine Software zur freien Nutzung zur Verfügung stellt, da damit das Risiko besteht, dass Kund*innen Zugriff auf den Quellcode und die Funktionsweise des Tools erhalten und diese unkontrolliert nutzen könnten. Es liegt nahe, dass schon zum Schutz von Unternehmensgeheimnissen der Betrieb im Wesentlichen durch die Mitarbeiter*innen erfolgt. Schließlich sprechen für umfassende Kenntnisse der Mitarbeiter*innen, dass bei anderen Unternehmen mit vergleichbaren Spionageangeboten (NSO-Group) Mitarbeiter*innen solche Kenntnisse bereits bestätigt haben.

Im vorliegenden Fall war ein Link gestaltet worden, der einer Teamseite eines Studierendenparlaments der […] University ähnelte. Dies spricht dafür, dass die Mitarbeiter*innen bei der Linkerstellung einen thematischen Bezug zur Anfrage einer Studierenden erkennen und daraus auch einen konkreteren Adressat*innenkreis folgern konnten. Schon wegen der wahrscheinlichen aktiven Einbindung von Mitarbeiter*innen in den Angriff in Kenntnis aller relevanten Umstände und der willentlichen Förderung und Ermöglichung ist ein Gehilf*innenvorsatz gegeben. Die obenstehenden Indizien sprechen dafür, dass die Mitarbeiter*innen sogar Kenntnis vom Anzeigeerstatter zu 1) als konkretes Angriffsziel hatten. Dies gilt umso mehr, da nach Angaben der Sicherheitsexpert*innen des Europäischen Parlaments nur der Anzeigeerstatter zu 1) eine Nachricht von der konkret genutzten E-Mail-Adresse erhielt.

Selbst wenn solche Kenntnisse der Mitarbeiter*innen nicht bestanden hätten, ergibt sich ein bedingter Gehilf*innenvorsatz schon aus dem Vertragsschluss bzw. der Leistungserbringung an die Haupttäter*innen, die die Software für illegale Zwecke auf deutschem Hoheitsgebiet einsetzten. So konnten die unmittelbaren unbekannten Täter*innen die Software und Services gegen einen in Deutschland aufhältigen Abgeordneten des EU-Parlaments einsetzen.

Das hochpreisige Tool mit seiner klaren Zielsetzung als Spionagesoftware stellten die Mitarbeiter*innen in Kenntnis seiner Nutzungsmöglichkeit und der konkret von den Kund*innen deutlich gemachten Nutzungswillen zur Verfügung und ergänzten es durch mögliche Personalisierungen und Angebotsanpassungen. Daneben ermöglichten sie auch den konkreten Angriff jedenfalls durch technisches Onboarding, Updates und Wartung. Den Mitarbeiter*innen waren dabei die weitreichenden invasiven Nutzungsmöglichkeiten der Software bekannt. Dennoch wurden Leistungen auch an Staaten wie Saudi-Arabien und Ungarn erbracht, obwohl bekannt war, dass diese sie illegal wie gegenüber dem Anzeigeerstatter zu 1) einsetzen. Dies gilt insbesondere für das wahrscheinliche Begehungsland Ungarn, in dem sowohl das Europäische Parlament als auch der Europäische Gerichtshof für Menschenrechte bereits gravierende Verletzungen von Menschenrechten durch Überwachungsmaßnahmen festgestellt haben.

Wie beim Angriff auf den Anzeigeerstatter zu 1) deutlich erkennbar, erbrachten die Mitarbeiter*innen der „Candiru Ltd." mit der Spionagesoftware Leistungen, die hohe Risiken mit sich bringen, ohne durch technische Mechanismen sicherzustellen, dass keine strafbare und grundrechtswidrige Nutzung erfolgt. Es besteht eine hohe Wahrscheinlichkeit, dass keine ausreichende Prüfung der Verlässlichkeit der Vertragspartner*innen, vorliegend wahrscheinlich der ungarischen Regierung, erfolgte oder ein Vertragsschluss trotz Kenntnis über die mangelnde Verlässlichkeit erfolgte. Es besteht daher eine hohe Wahrscheinlichkeit, dass sich die unbekannten Mitarbeiter*innen bei Vergabe der Software damit abfanden und einkalkulierten, dass Kund*innen die Software und Services in strafbarer und rechtsstaatswidriger Weise einsetzen würden, wie es im konkreten Fall im deutschen Inland und insbesondere gegen einen Abgeordneten des Europäischen Parlaments erfolgt ist. Damit nahmen die Mitarbeiter*innen mit hoher Wahrscheinlichkeit billigend in Kauf, dass durch die vertragliche Überlassung der Software und die Serviceangebote Spyware-Angriffe wie die vorliegende Haupttat ermöglicht werden.

Zum Zeitpunkt des Verkaufs der Spähprogramme war es zwar unter Umständen noch nicht gesichert, dass der Anzeigenerstatter zu 1) Angriffsziel werden sollte. Nach der Rechtsprechung muss sich der Gehilfenvorsatz nur auf eine in ihren wesentlichen Merkmalen und Grundzügen konkretisierten Tat richten (BGH, Urteil vom 29. November 2006 – 2 StR 301/06, juris Rn. 8), und damit gerade nicht alle Einzelheiten und Details umfassen (TK-StGB/*Weißer*, 31. Aufl. 2025, StGB § 27 Rn. 41). Anders als bei der Anstiftung, bei der Anstifter*innen eine bestimmten Taterfolg vor Augen haben, erbringen Gehilf*innen einen von der Haupttat losgelösten Beitrag (BGH, Urteil vom 18. April 1996 – 1 StR 14/96, juris Rn. 12). Daher reicht es aus, wenn der Gehilfe dem Täter ein entscheidendes Tatmittel willentlich an die Hand gibt und damit bewusst das Risiko erhöht, dass eine durch den Einsatz gerade dieses Mittels typischerweise geförderte Haupttat verübt wird (BGH, Urteil vom 18. April 1996 – 1 StR 14/96, juris Rn. 2). Folglich ist es unschädlich, dass den Gehilfen eventuell nicht im Einzelnen klar war, um welchen Betroffenen es sich genau handeln würde.

bb) Keine neutrale Beihilfe

Die Überlassung der Spionagesoftware ist bereits nicht als neutrale Handlung anzusehen, da es sich hier um die Zurverfügungstellung eines hochinvasiven Angriffsmittels handelt, bei dessen Herstellung und Verkauf nicht ohne weiteres davon ausgegangen werden kann, dass ein rechtmäßiger Einsatz möglich ist oder ausschließlich ein gesetzeskonformer Einsatz erfolgt. Der Einsatz von Spyware ist grundsätzlich nur für staatliche Stellen und nur in engen Grenzen zulässig. Die Verschaffung und der Betrieb von so weitgehenden Spionagetools wie „Candiru" ist schon kein sozialtypisches, neutrales alltägliches und professionell adäquates Verhalten und keine gewöhnliche Softwaredienstleistung. Das ergibt sich vorrangig aus den weitreichenden Spähmöglichkeiten, die hochinvasive Eingriffe in Art. 10 GG und das IT-Grundrecht beinhalten. Bei dem Softwareangebot handelt es sich zudem nicht um eine einfach zu lizensierende Standardsoftware, sondern um ein Service-Angebot, das mithilfe eines hochpreisigen und nicht ohne weiteres erhältlichen Tools erbracht wird. Hinzukommt, dass die Spionageangebote von „Candiru Ldt." auf Kund*innenwunsch hin angepasst, insbesondere Services hinzugebucht werden können und höchstwahrscheinlich eine konkrete Anzahl von Spyware-Angriffen und eine unbegrenzte Zahl von Versuchen vertraglich zugesichert wird. Unter den bekannten Kund*innen von „Candiru Ldt." befinden sich mit Saudi-Arabien, den Vereinigten Arabischen Emiraten und Ungarn mit hoher Wahrscheinlichkeit mehrere, bei welchen starke Anhaltspunkte dafür bestanden und bestehen, dass ein Einsatz nicht nur in

rechtsstaatlichen Grenzen und insbesondere in anderen Staaten zum Angriff auf Regierungskritiker*innen genutzt wird. In Ungarn ist nicht durch rechtliche Rahmenbedingungen sichergestellt, dass Spähsoftware menschenrechtskonform eingesetzt wird.

Selbst wenn man den Verkauf einer solchen Software als berufstypische oder neutrale Handlung ansieht und daher eine Beihilfestrafbarkeit nur unter engen Voraussetzungen zulässt, sind diese Voraussetzungen gegeben. Für berufstypische, neutrale Handlungen zieht die Rechtsprechung einschränkend bestimmte Grundsätze heran: Zielt das Handeln der Haupttäter*innen ausschließlich darauf ab, eine strafbare Handlung zu begehen, und weiß dies der Hilfeleistende, so ist sein Tatbeitrag als Beihilfehandlung zu werten. In diesem Fall ist die Handlung als „Solidarisierung“ mit den Täter*innen zu deuten und dann auch nicht mehr als „sozialadäquat“ anzusehen (BGH, Beschluss vom 20. September 1999 – 5 StR 729/98, juris Rn. 18). Auch ohne sicheres Wissen reicht ein erkennbar hohes Risiko strafbaren Verhaltens aus, wenn das Risiko derart hoch ist, dass der*die Gehilf*in sich mit seiner Unterstützung „die Förderung der erkennbar tatgeneigten Täter […] angelegen sein“ lässt (BGH, Urteil vom 26. Oktober 1998 – 5 StR 746/97, juris Rn. 49).

Von einem erkennbar hohen Risiko strafbaren Verhaltens ist bei dem Verkauf einer so hochinvasiven Spionagesoftware wie der von „Candiru Ldt.“ auszugehen, da eine Infiltration ohne jegliche Mitwirkung (zero-click) erfolgen kann und der Einsatz von Spyware Zugang zu intimsten und sensibelsten Informationen ermöglicht, die für Straftäter*innen von hohem Interesse sind. Mit der Überlassung eines Spionagetools wie „Candiru“ ließen sich die Mitarbeiter*innen die Förderung der Straftaten der unbekannten Täter*innen erkennbar angelegen sein.

Auch besteht zumindest die Wahrscheinlichkeit, dass Mitarbeiter*innen der „Candiru Ltd.“ aufgrund weitreichender Zugriffsmöglichkeiten sichere Kenntnis vom Angriff auf den Anzeigeerstatter zu 1) hatten, sodass auch aus diesem Grunde eine strafbare Beihilfe gegeben wäre.

d) Strafantrag

Auch bezüglich der unbekannten Mitarbeitenden wird der nach § 205 Abs. 1 StGB erforderliche Strafantrag gestellt.

2. § 202c Abs. 1 Nr. 2 StGB

Weiterhin kommt durch den Verkauf der Software an Vertragspartner*innen, durch die die unbekannten Täter*innen diese gegen den Anzeigeerstatter zu 1) einsetzen konnten, mit hoher Wahrscheinlichkeit eine Strafbarkeit gemäß § 202c Abs. 1 Nr. 2 Var. 1, 2 StGB in Betracht.

Zur Anwendbarkeit des deutschen Strafrechts und zur Tatbestandsverwirklichung kann auf die Ausführungen unter I. 3. verwiesen werden.

3. §§ 303a Abs. 1, 2, 22, 23 Abs. 1, 27 StGB bzw. §§ 303a Abs. 3 i.V.m. § 202c Abs. 1 Nr. 2 StGB und §§ 303b Abs. 1, 2, 3, 22, 23 Abs. 1, 27 StGB bzw. § 303b Abs. 5 i.V.m. § 202c Abs. 1 Nr. 2 StGB

Mit hoher Wahrscheinlichkeit haben sich die unbekannten Mitarbeiter*innen der „Candiru Ltd.“ auch wegen Beihilfe zur versuchten Datenveränderung sowie zur versuchten Computersabotage strafbar gemacht.

Jedenfalls stellt das Verschaffen der Software der „Candiru Ltd." eine strafbare Vorbereitung solcher Taten im Sinne von §§ 303b Abs. 1, 2, 3, 22, 23 Abs. 1 StGB und § 303b Abs. 5 i.V.m. § 202c Abs. 1 Nr. 2 StGB dar.

Auch diesbezüglich werden die erforderlichen Strafanträge gestellt.

III. Anfangsverdacht gegen ungarische Regierungsverantwortliche, insbesondere Viktor Orbán

Der Spyware-Angriff auf den Anzeigeerstatter zu 1) erfolgte mit hoher Wahrscheinlichkeit auf Anordnung bzw. Befehl staatlicher Organisationen. Dies liegt schon deshalb nahe, da mit hoher Wahrscheinlichkeit nur Regierungen Kund*innen der „Candiru Ltd." sind.

Es bestehen konkrete Anhaltspunkte, dass der konkrete Angriff von ungarischen Behörden verübt wurde. Der Anzeigeerstatter zu 1) engagiert sich als Abgeordneter des Europäischen Parlaments für Rechtsstaatlichkeit in der Europäischen Union und insbesondere in Ungarn. Dies stellt einen Schwerpunkt seiner Tätigkeiten als Abgeordneter dar. Er kritisiert rechtsstaatswidrige Handlungen der ungarischen Regierung, insbesondere Viktor Orbán. Seine Arbeit trug insbesondere stark dazu bei, dass durch den Rat auf Vorschlag der Europäischen Kommission eine Anwendung der Konditionalitätsverordnung und damit Sanktionen für Ungarn beschlossen wurden. Aufgrund seines starken Einsatzes in diesem Bereich und mangels Engagements zu anderen Staaten sind Spionageangriffe aus Ungarn als wahrscheinlich und Angriffe aus anderen Staaten als unwahrscheinlich anzusehen. Dies gilt umso mehr, da der Anzeigeerstatter zu 1) nach Auskunft der Sicherheitsexpert*innen des Europäischen Parlaments der einzige Abgeordnete war, der mit der genutzten Mail-Adresse angegriffen wurde.

Aus diesem Grunde besteht eine hohe Wahrscheinlichkeit dafür, dass die Angriffe von ungarischen Regierungsverantwortlichen angeordnet wurden. Daher kommen Minister*innen und andere Leiter*innen von Behörden als möglicher Mittäter*innen, mittelbare Täter*innen kraft Organisationsherrschaft sowie Anstifter*innen zu den dargestellten Straftaten der unbekannten Täter*innen in Betracht.

Dies gilt im besonderen Maße für den ungarischen Ministerpräsident Viktor Orbán. Dieser hat Daniel Freund in der Vergangenheit bereits herausgehoben und als einzigen Abgeordneten im Rahmen einer Rede im Europäischen Parlament verbal angegriffen und ihm insbesondere Korruption vorgeworfen. Aus diesem Grunde kann zumindest vermutet werden, dass der Ministerpräsident Spionageangriffe auf den Anzeigeerstatter zu 1) angeordnet oder verlangt hat.

Aber auch die Beteiligung anderer Behördenleiter*innen ist wahrscheinlich. Der Spionageangriff auf einen ausländischen EU-Abgeordneten fällt mit hoher Wahrscheinlichkeit in den Zuständigkeitsbereich des ungarischen Auslandsgeheimdienst Információs Hivatal (Intelligence Office). Dieser wird von […] geleitet. Die nationalen Sicherheitsbehörden unterstehen zudem dem Minister und Leiter des Kabinettsbüros des Ministerpräsidenten, […]. Aber auch eine Genehmigung durch den damaligen Justizminister, […], erscheint nicht unwahrscheinlich.

Der gestellte Strafantrag erstreckt sich daher auch auf eine mögliche Strafbarkeit dieser genannten und weiterer Personen. Die Frist des § 77b Abs. 2 StGB ist insoweit nicht verstrichen, da die Verantwortlichen für den Anzeigeerstatter zu 1) und Antragssteller nicht sicher bekannt sind, es handelt sich vielmehr um bloße Vermutungen, die noch keinen Fristbeginn auslösen (*Kindhäuser/Hilgendorf*, StGB, 10. Aufl. 2025, StGB § 77b Rn. 2).

D. Mögliche Ermittlungsmaßnahmen

Wir regen an, den Sachverhalt durch die nachfolgenden Ermittlungsmaßnahmen weiter aufzuklären:

I. Vernehmungen

Von Zeug*innen:

Zum Tathergang:

Daniel Freund

[…]Von sachverständigen Zeugen zur Spionagesoftware:

Mitarbeitende der Cybersecurity Operations Unit des Europäischen Parlaments
[…]

II. Analysen

Forensische Analyse des EP Parlaments zum zugesandten Link

Marczak/Scott-Railton/Berdan et al: Hooking Candiru, Bericht des Citizen Labs zu Candiru, abrufbar unter https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

Durchführung einer eigenständen Analyse

III. Amtshilfeersuchen/Behördenauskünfte

Den Anzeigeerstattenden ist zwar nicht bekannt, ob die unten aufgeführten Ansprechstellen die infragestehenden Spähprogramme nutzen. Angesichts ihres Arbeitsauftrags ist aber davon auszugehen, dass sie Einblicke in die Funktionsweise der Programme und die Informationszugänge, Services und Steuerungsmöglichkeiten der Unternehmen und ihrer Mitarbeiter*innen haben und sich bereits mit ihnen auseinandergesetzt haben.

Das sind im Einzelnen:

Bundesamt für Verfassungsschutz
+49(0)228 99 792-0; 030 18 792-0; poststelle@bfv.bund.de

Bundesnachrichtendienst
030 414 64 57; zentrale@bnd.bund.de oder poststelle@bnd.bund.de

Zentrale Stelle für Informationstechnik im Sicherheitsbereich
089 / 6 08 06 79 – 0; poststelle@zitis.bund.de

Bundesamt für Sicherheit in der Informationstechnik
+49 228 99 9582-0; bsi@bsi.bund.de

Es wird um eine Eingangsbestätigung sowie um die Mitteilung eines Aktenzeichens gebeten.

Mit freundlichen Grüßen

Daniel Freund	Malte Spitz, Gesellschaft für Freiheitsrechte e.V.
Brüssel, den	Berlin, den

Anlage 1

[…]