Europäisches Parlament
2019-2024

Plenarsitzungsdokument

A9-0189/2023

22.5.2023

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 (2022/2077(INI))

Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware

Berichterstatterin: Sophie in ‘t Veld

INHALT

Seite

VORLÄUFIGE ERGEBNISSE

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
(2022/2077(INI))

Das Europäische Parlament,

– gestützt auf Artikel 226 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV),

– gestützt auf seinen Beschluss vom 10. März 2022 über die Einsetzung, die Zuständigkeiten, die Mitgliederzahl und die Mandatszeit des Untersuchungsausschusses zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware und die Festlegung des Gegenstands der Untersuchung,

– gestützt auf Artikel 54 und 208 seiner Geschäftsordnung,

– unter Hinweis auf den Bericht des Untersuchungsausschusses zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (A9-0189/2023).

Allgemeine Einleitung

1. Im Juli 2021 veröffentlichte ein Konsortium von Investigativjournalisten, NGOs und Forschern – das Pegasus-Projekt – einen Bericht auf der Grundlage einer Liste, die in ihren Besitz gelangt war und etwa 50 000 Telefonnummern aufführt, bei denen es sich um potentielle Ziele der Spähsoftware Pegasus handelte. Die Spähsoftware wurde sowohl von autoritären als auch demokratischen Regierungen auf der ganzen Welt, sowohl mit als auch ohne gerichtliche Kontrolle, gegen Journalisten, Anwälte, Richter, Aktivisten, Politiker und Staatsbeamte eingesetzt. Auch in der Europäischen Union wurden Menschen Opfer von Angriffen mit Spähsoftware: Diese gingen sowohl von Akteuren außerhalb der EU als auch von Akteuren innerhalb der EU, einschließlich der Regierungsbehörden, aus. Die meisten, wenn nicht alle Regierungen der Mitgliedstaaten haben Spähsoftware zu Strafverfolgungs- und Sicherheitszwecken erworben. Es gibt jedoch reichlich Beweise dafür, dass Spähsoftware in mehreren Mitgliedstaaten zu rein politischen Zwecken missbraucht wurde und sich gegen Kritiker und Gegner der regierenden Parteien richtete oder im Zusammenhang mit Korruption eingesetzt wurde. Untersuchungsergebnisse fanden Verbindungen von Pegasus und anderer Überwachungs-und Spähsoftware zu verschiedenen Menschenrechtsverletzungen durch Regierungen, darunter Überwachung, Erpressung, Verleumdungskampagnen, Einschüchterung und Belästigung. Dies wirft auf verschiedenen Ebenen der EU-Rechtsordnung Bedenken hinsichtlich des Datenschutzes und der Privatsphäre, der Meinungsfreiheit, der Pressefreiheit, der Vereinigungsfreiheit, der Rechtsbehelfe, der Rechtsmittel und des fairen Verfahrens sowie der demokratischen Prozesse und Institutionen auf. Obwohl der Einsatz von Spähsoftware im Falle schwerwiegender Bedrohungen der nationalen Sicherheit erforderlich und angemessen sein kann, ist der Missbrauch von Spähsoftware für politische Zwecke äußerst besorgniserregend und

wirft sehr ernste Bedenken hinsichtlich der verfahrensrechtlichen und materiellen Rechtmäßigkeit der Überwachungspraktiken und des durch das europäische und nationale Recht gewährten Schutzniveaus auf. Ein solcher Missbrauch von Spähsoftware untergräbt unmittelbar die Grundwerte, auf denen die EU gründet, nämlich die Grundrechte und die Demokratie. Die nachfolgenden investigativen Medienberichte und andere Quellen haben gezeigt, dass Überwachungs- und Spähsoftware aus EU-Ländern in Drittländer mit undemokratischen Regime und einem hohen Risiko von Menschenrechtsverletzungen exportiert wird, was offensichtlich gegen die EU-Ausfuhrvorschriften verstößt. Die Spähsoftware-Industrie ist in der EU fest etabliert und profitiert von sehr günstigen Bedingungen für Unternehmen.

2. Als Reaktion auf diesen sich ausweitenden Skandal beschloss das Europäische Parlament am 10. März 2022, einen Untersuchungsausschuss gemäß Artikel 226 AEUV einzusetzen, um behauptete Verstöße oder Missstände bei der Anwendung des Unionsrechts in Bezug auf den Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware zu prüfen („PEGA“). Als Verstoß wird das Vorliegen eines rechtswidrigen Verhaltens, entweder durch Handlungen oder Unterlassungen, die gegen das Gesetz verstoßen, seitens der Organe oder Einrichtungen der Union oder der Behörden der Mitgliedstaaten bei der Umsetzung und Durchsetzung des EU-Rechts bezeichnet, als Missstände bei der Anwendung werden unzureichende oder fehlende Verwaltungsmaßnahmen bezeichnet, beispielsweise, wenn die Grundsätze der guten Verwaltung nicht eingehalten werden. Beispiele für Missstände bei der Anwendung sind Unregelmäßigkeiten und Unterlassungen, Machtmissbrauch, Ungerechtigkeit, Funktionsstörungen oder Inkompetenz, Diskriminierung, aber auch vermeidbare Verzögerungen, Verweigerung der Bereitstellung von Informationen, Nachlässigkeit und andere Mängel, die auf eine mangelhafte Anwendung des Unionsrechts schließen lassen.

3. Für die Zwecke dieser Untersuchung hat PEGA einen breiten Definitionsbereich für Spähsoftware verwendet, der jegliche Spähsoftware umfasst, die auf mobilen Geräten durch Ausnutzung von IT-Schwachstellen installiert wird. Während der Untersuchung wurde auch die in der Dual-Use-Verordnung festgelegte Definition des Begriffs „Güter für digitale Überwachung“ verwendet: diese Definition beschreibt sie als „Güter mit doppeltem Verwendungszweck, die besonders dafür konstruiert sind, die verdeckte Überwachung natürlicher Personen durch Überwachung, Extraktion, Erhebung oder Analyse von Daten aus Informations- und Telekommunikationssystemen zu ermöglichen“. Im September 2022 schlug die Kommission in ihrem Vorschlag für ein Medienfreiheitsgesetz folgende Definition für Spähsoftware vor: „jedes Produkt mit digitalen Elementen, das speziell dafür ausgelegt ist, Schwachstellen in anderen Produkten mit digitalen Elementen auszunutzen, und das die verdeckte Observierung natürlicher oder juristischer Personen durch Überwachung, Extraktion, Sammlung oder Analyse von Daten aus solchen Produkten oder von natürlichen oder juristischen Personen, die solche Produkte verwenden, ermöglicht, insbesondere durch geheime Aufzeichnung von Anrufen oder anderweitige Nutzung des Mikrofons eines Endgeräts, durch das Filmen natürlicher Personen, Maschinen oder ihrer Umgebung, durch das Kopieren von Nachrichten, durch Fotos, Verfolgung der Surftätigkeiten im Browser, Verfolgung von Geolokalisierungsdaten, Erhebung anderer Sensordaten oder Verfolgungstätigkeiten über mehrere Endnutzergeräte hinweg, ohne dass die betreffende natürliche oder juristische Person konkret informiert wird und ihre

ausdrückliche Einwilligung hierzu gegeben hat."

4. Am 19. April 2022 begann die PEGA mit ihrer Arbeit und sammelte Informationen durch öffentliche Anhörungen, Informationsreisen, Anhörung von Sachverständigen, Anfragen von Daten, Beweismittel und Recherche.

5. Bei mehreren öffentlichen Anhörungen prüfte der Untersuchungsausschuss die Funktionsweise von Spähsoftware. Spähsoftware ist eine Art von Schadsoftware, die die Aktivitäten von Benutzern ohne ihr Wissen oder ihre Zustimmung überwacht. Eine solche Überwachung kann Keylogger, Aktivitätsüberwachung und Datenerfassung sowie andere Formen von Datendiebstahl umfassen. Spähsoftware wird in der Regel als Trojaner oder durch Ausnutzung von Software-Schwachstellen verbreitet[1]. Spähsoftware kann aus der Ferne auf den Mobiltelefonen von vorab identifizierten Personen installiert werden, auch über Grenzen hinweg. In einigen Fällen werden Telekommunikationsnetze für die Übertragung der Spähsoftware an das Zielgerät verwendet. Sobald die Spähsoftware das System infiltriert hat, deaktiviert sie Schutzmechanismen und Sicherheitsupdates. Das infizierte Gerät überträgt dann die gesammelten Daten und ermöglicht eine Echtzeitüberwachung, bei der eingehende Textnachrichten gelesen, Anrufe und Standorte verfolgt und Audio und Video über das Mikrofon und die Kamera des Geräts aufgerufen und aufgenommen werden.

6. Im Gegensatz zum herkömmlichen Abhören, das nur die Echtzeitüberwachung der Kommunikation ermöglicht, kann Spähsoftware einen vollständigen, rückwirkenden Zugriff auf Dateien und Nachrichten, die in der Vergangenheit erstellt wurden, Passwörter und Metadaten über frühere Kommunikationsvorgänge ermöglichen. Infolgedessen bieten ein gerichtlich festgelegter Beginn und Zeitraum einer Überwachungsaktion keinen ausreichenden Schutz, wenn Spähsoftware einen vollständigen rückwirkenden Zugriff auf Daten gewährt. Außerdem ist es Verwendern technisch möglich, sich als die Zielperson auszugeben, indem sie sich Zugang zu ihren digitalen Anmeldedaten und ihrer Identität verschaffen. Es ist äußerst schwierig für die betroffene Person zu erkennen, ob sie Opfer eines Angriffs mit Spähsoftware wurde. Spähsoftware hinterlässt wenige oder keine Spuren auf dem Zielgerät, und selbst wenn sie erkannt wird, ist es sehr schwierig festzustellen, wer für den Angriff verantwortlich war.

7. PEGA hat von den nationalen Behörden wenige oder keine Antworten über den Erwerb und den Einsatz von Spähsoftware in ihren Mitgliedstaaten oder über diesbezügliche Haushaltsaspekte erhalten. Die Anbieter und Länder, die Exportlizenzen ausstellen (in den meisten Fällen Israel) teilen keine Informationen über ihre Kunden. Viele Behörden der Mitgliedstaaten stellten PEGA keine aussagekräftigen Informationen über die rechtlichen Rahmenbedingungen für den Einsatz von Spähsoftware oder über den Einsatz von Spähsoftware in ihren Mitgliedstaaten bereit, die über das hinausgingen, was bereits öffentlich bekannt war, hauptsächlich aufgrund nationaler rechtlicher Anforderungen in Bezug auf Geheimhaltung und Vertraulichkeit.

8. Einige Mitgliedstaaten haben Spähsoftware eingesetzt und sich geweigert, sich dazu zu äußern, indem sie sich auf die nationale Sicherheit berufen, die nach Artikel 4 Absatz 2 des Vertrags über die Europäische Union (EUV) „weiterhin in die alleinige

[1] https://www.enisa.europa.eu/topics/incident-response/glossary/malware.

Verantwortung der einzelnen Mitgliedstaaten [fällt]“. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) und des Europäischen Gerichtshofs für Menschenrechte (EGMR) müssen nationale Sicherheitserwägungen jedoch mit den im EU-Recht verankerten Grundrechten und demokratischen Normen in Einklang gebracht werden. Obwohl es Sache der Mitgliedstaaten ist, ihre wesentlichen nationalen Sicherheitsinteressen zu definieren und geeignete Maßnahmen zur Gewährleistung ihrer inneren und äußeren Sicherheit zu ergreifen, entschied der EuGH, dass „die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht dazu führen [kann], dass das Unionsrecht unanwendbar ist und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbunden werden[2]“, und stellte klar, welche Kriterien die Mitgliedstaaten bei der Festlegung von Fragen, die unter die nationale Sicherheit fallen, zu beachten haben. Mehrere Mitgliedstaaten haben geltend gemacht, dass der Einsatz von Spähsoftware unter die nationale Sicherheit falle und dass dies die Anwendbarkeit des EU-Rechts ausschließe. Wenn die Mitgliedstaaten jedoch nur einen bloßen Verweis auf die nationale Sicherheit als solche vorbringen, kann die Beschränkung der Grundrechte nicht als unter die nationale Sicherheit fallend gerechtfertigt werden. Das EU-Recht muss mit allen Garantien, die es bietet, Anwendung finden. Es gibt reichlich Beweise für einen Missbrauch von Spähsoftware aus Gründen, die in keinem Zusammenhang mit der nationalen Sicherheit stehen. Die Mitgliedstaaten sollten nicht durch einen bloßen Verweis auf die nationale Sicherheit in der Lage sein, der Rechenschaftspflicht für solche schwerwiegenden Missbräuche von Spähsoftware zu entgehen. Aufgrund dieser Unklarheit war es schwierig, ausreichende Informationen während Anhörungen und Informationsreisen sowie durch Informationsanfragen zu erhalten. Die mangelnde Klarheit darüber, wie die nationale Sicherheit definiert wird, und die übermäßig weite Auslegung ihres Anwendungsbereichs durch die nationalen Behörden stellen eine Herausforderung dar, wenn es darum geht, die Rechtfertigung für den Einsatz von Spähsoftware zu verstehen.

9. Durch die Zusammenstellung von Informationen aus verschiedenen Quellen konnte PEGA jedoch ein zwar unvollständiges, aber klares Bild rekonstruieren und Probleme identifizieren, die Anlass zu Besorgnis geben und weitere Untersuchungen verdienen.

10. Es kann mit Sicherheit angenommen werden, dass die Behörden in allen Mitgliedstaaten Spähsoftware in irgendeiner Weise, ob rechtmäßig oder unrechtmäßig, einsetzen. Spähsoftware kann direkt oder über einen Stellvertreter, ein Maklerunternehmen oder einen Zwischenhändler erworben werden. Statt die Software tatsächlich zu erwerben, können auch Vereinbarungen über bestimmte Dienstleistungen geschlossen werden. Zusätzliche Dienstleistungen können angeboten werden, wie die Schulung von Personal oder die Bereitstellung von Servern. Spähsoftware ist nicht isoliert zu betrachten, sondern als Teil einer großen Bandbreite von Produkten und Dienstleistungen, die auf einem expandierenden und lukrativen globalen Markt angeboten werden. Wichtig ist, sich zu vergegenwärtigen, dass der Erwerb und die Nutzung von Spähsoftware sehr kostspielig ist und sich auf Millionen von Euro beläuft. In vielen Mitgliedstaaten wird diese Ausgabe jedoch nicht im regulären Haushalt

[2] Urteil vom 6. Oktober 2020, *Privacy International/ Secretary of State for Foreign and Commonwealth Affairs u. a.*, C-623/17, EU:C:2020:790.

ausgewiesen, wodurch Kontrollen umgangen werden können.

11. Aus Informationen der NSO Group geht hervor, dass Pegasus bis zur Beendigung der Verträge mit zwei Ländern in mindestens 14 EU-Ländern verkauft wurde. Es ist nicht bekannt, um welche Länder es sich dabei handelt, doch die allgemeine Annahme lautet, dass es Polen und Ungarn sind. Solange die NSO Group oder die israelische Regierung jedoch keine offizielle Erklärung über eine Vertragsbeendigung abgeben, kann dies nicht überprüft werden.

12. Eine weitere Information ist die Teilnehmerliste aus dem Jahr 2013 der Konferenz ISS (Intelligence Support Systems)World, auch bekannt als „The Wiretappers Ball“. Mit Ausnahme von Portugal und Luxemburg waren alle derzeitigen EU-Mitgliedstaaten durch eine Vielzahl von Organisationen vertreten, darunter lokale Polizeikräfte[3]. In den letzten Jahren ist die NSO Group der Hauptsponsor der Veranstaltung geworden, aber die Sponsorenliste umfasst neben vielen anderen auch Intellexa, Candiru und RCS[4].

13. Die Mitgliedstaaten sind nicht nur Kunden der gewerblichen Anbieter von Spähsoftware, sondern spielen auch andere, unterschiedliche Rollen im Handel mit Spähsoftware. In einigen Mitgliedstaaten haben Anbieter von Spähsoftware ihren Sitz, einige sind beliebte Standorte für Finanz- und Bankdienstleistungen, und andere bieten Akteuren der Branche die Staatsbürgerschaft an oder gewähren ihnen Aufenthalt.

14. In der überwiegenden Mehrheit der Mitgliedstaaten werden Nachrichtendienste durch einen Rechtsrahmen geregelt – häufig mit Bestimmungen über die Organisation und Funktionsweise dieser Dienste sowie ihre Aufträge und Befugnisse, einschließlich ihrer Handlungsmöglichkeiten und Bedingungen für ihren Einsatz – sowie durch Aufsichtsmechanismen, die Exekutivkontrolle, parlamentarische Aufsicht, Expertengremien und gerichtliche Überprüfung umfassen. Dennoch wurden Bedenken hinsichtlich der permissiven Rahmenbedingungen für die Nachrichtendienste, der unwirksamen Kontrollen, der laxen Aufsichtspraktiken sowie der politischen Einmischung bestimmter Länder geäußert**.**

15. Spähsoftware wird eindeutig auch von den Vollzugsbehörden verwendet, nicht nur von Nachrichtendiensten. Es bestehen ernsthafte Bedenken hinsichtlich der Zulässigkeit solchen Materials als Beweismittel vor Gericht im Rahmen der polizeilichen und justiziellen Zusammenarbeit der EU, auch innerhalb von Europol und Eurojust, wenn diese Informationen aus Ermittlungsmethoden stammen, die ohne ordnungsgemäße gerichtliche Kontrolle angewandt wurden. Je nach den nationalen Rechtsvorschriften ist der Einsatz von Spähsoftware bei Ermittlungen unter richterlicher Aufsicht rechtmäßig.

16. Der Missbrauch von Spähsoftware ist eine Bedrohung für die Demokratie und die Grundrechte. Seit den Enthüllungen des Pegasus-Projekts haben die Vereinigten Staaten mehrere Schritte unternommen, um den Missbrauch von Spähsoftware zu untersuchen und zu regulieren. Innerhalb der EU gab es in diesem Bereich bisher nur sehr wenige Maßnahmen. Es müssen klare Regeln für Einsatz von und den Handel mit Spähsoftware festgelegt werden, vorzugsweise zusammen mit anderen Ländern wie den USA.

[3] https://wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf.
[4] https://www.issworldtraining.com/iss_europe/sponsors.html.

I. Die Verwendung von Spähsoftware in der EU

I.A Polen

17. Die Vertreter der Ministerien lehnten ein Treffen mit der Delegation des Ausschusses ab. In dem von PEGA am 15. Juli 2022 übermittelten Fragebogens beantworteten die polnischen Behörden nicht alle Fragen und bestanden darauf, dass die bestehenden Bestimmungen ausreichend seien und dass sie streng im Rahmen des Gesetzes tätig seien[5]. Der Innenminister Mariusz Kaminski weigerte sich ebenfalls, eine Einladung von PEGA zum Meinungsaustausch anzunehmen[6].

18. Die Informationsreise von PEGA nach Polen im September 2022 war für den Ausschuss von größter Bedeutung und ermöglichte es ihm, Informationen und Fakten über den Einsatz der Spähsoftware Pegasus zu sammeln. Die Treffen in Warschau werfen ein neues Licht auf den illegalen Einsatz von Überwachungssoftware gegen demokratische Akteure in Polen. Die Mitglieder erfuhren, wie das System der rechtlichen und institutionellen Gewaltenteilung abgebaut wurde, um den Angriff von Einzelpersonen, die als politische Gegner gelten, mit Cyberwaffen auf militärischem Niveau zu ermöglichen. Infolgedessen wurden wichtige demokratische Standards und Bürgerrechte, die in den Rechtsvorschriften der EU und Polens verankert sind, grob verletzt. Dies ist eine weitere Dimension der Krise der Rechtsstaatlichkeit in Polen.

ERWERB VON PEGASUS

19. Im November 2016 nahmen die ehemalige Ministerpräsidentin und derzeitiges Mitglied im Europäischen Parlament, Beata Szydło, und der ehemalige Außenminister Witold Waszczykowski an einem Abendessen im Haus des damaligen israelischen Premierministers Benjamin Netanjahu teil[7]. Im darauffolgenden Jahr, im Juli, trafen sich Szydło und Netanjahu mit den Regierungschefs der Länder der Visegrád-Gruppe. Angeblich sprachen sie über die „Stärkung der Zusammenarbeit im Bereich der Innovation und der Hochtechnologien“ und über „Fragen im Zusammenhang mit der Sicherheit der Bürger im weiteren Sinne“[8]. Kurz nach diesem Treffen im Jahr 2017 wurde Pegasus nach einem Treffen zwischen Premierminister Mateusz Morawiecki, dem ungarischen Premierminister Viktor Orbán und Netanjahu von der polnischen Regierung erworben[9].

20. Zunächst bestritten die polnische Regierung und der PiS-Chef Jarosław Kaczyński den Erwerb von Pegasus[10]. Anfang Januar 2022 bestätigten sie jedoch den Erwerb von

---

[5] Antwort des Ständigen Vertreters Polens bei der EU, Andrzej Sadós, an den PEGA-Ausschuss, 7. September 2022.
[6] Antwort von Innenminister Mariusz Kaminski mit Schreiben an den PEGA-Ausschuss vom 12. Juli 2022.
[7] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29. Januar 2022.
[8] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29 January 2022.
[9] Financieele Dagblad, ‘De wereld deze week: het beste uit de internationale pers’, 7 January 2022.
[10] https://www.politico.eu/article/poland-government-scrambles-minimize-hacking-backlash/.

Spähsoftware durch die polnische Regierung[11][12][13]. Im selben Monat wurde festgestellt, dass der Oberste Rechnungshof 2018 im Rahmen einer Prüfung des Justizfonds, die vom Justizministerium betrieben und zur Unterstützung von Opfern von Straftaten eingerichtet wurde, wichtige Beweise im Zusammenhang mit dem Erwerb von Pegasus gesammelt hatte. Am 18. Januar 2022 sagte der ehemalige Chef des Obersten Rechnungshofs Polens (NIK) und später unabhängige Senator Krzysztof Kwiatkowski vor dem außerordentlichen Ausschuss des Senats für Überwachungsfälle unter Einsatz des Pegasus-Systems zu dem Erwerb von Pegasus aus[14]. Nachdem er von der Geheimhaltungspflicht im Zusammenhang mit seiner Position befreit wurde, legte er dem Ausschuss zwei Rechnungen vor, die den Erwerb von Spähsoftware für das Zentrale Antikorruptionsbüro (CBA) bestätigen, wobei 25 Mio. PLN aus dem Justizfonds des Justizministeriums stammten[15]. Kwiatkowski bezeugte, dass der NIK Konten der polnischen Nationalbank entdeckt habe, die die Überweisung bescheinigten[16].

21. Die Rechnungen wurden von der Matic Sp. z o.o. ausgestellt, die als Vermittlerin fungierte und diesen Erwerb für das CBA durchführte[17]. Die Matic Sp. z o.o. ist ein IT- und Sicherheitsunternehmen mit Sitz in Warschau, dessen Eigentümer und Betreiber Personen sind, die zu Zeiten des Kommunismus im Nachrichten- und Sicherheitsdienst tätig waren[18].

22. Matic wurde unmittelbar nach dem Erwerb von Pegasus im November 2017 zu einer Aktiengesellschaft und ist laut der Tageszeitung Gazeta Wyborcza mit einer Genehmigung des Innenministeriums im Handel mit Technologien mit den Sicherheitsdiensten und der Polizei sowie im Waffenhandel tätig.[19]Das Unternehmen besitzt auch ein spezielles Lizenzzertifikat der Agentur für innere Sicherheit, das diese 2019 ausgestellt hat und das es dem Unternehmen erlaubt, bestimmte vertrauliche Informationen bis zum Ende des Jahrzehnts geheim zu halten[20]. Vertreter von Matic lehnten ein Treffen und den Informationsaustausch mit dem Untersuchungsausschuss ab.

---

[11] Financieele Dagblad, ‘Liberalen Europarlement eisen onderzoek naar spionagesoftware’, 12 January 2022.
[12] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/.
[13] January 2022, Financial Times, https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e, 8 February 2022.
[14] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 January 2022.
[15] ONET, https://wiadomosci.onet.pl/kraj/wiceminister-michal-wos-nie-wiem-co-to-jest-pegasus/e9fbrvh, 3 January 2022; Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 January 2022.
[16] The Wire, https://thewire.in/world/poland-audit-office-invoice-pegasus-purchase-reopen-investigation, 4 January 2022; Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 January 2022.
[17] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 January 2022.
[18]https://ipn.gov.pl/en/about-the-institute.
[19] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 January 2022.
[20] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 January 2022.

23. Nach polnischem Recht können die Tätigkeiten des CBA nur aus dem Staatshaushalt finanziert werden. Der Erwerb von Pegasus wurde jedoch aus dem Justizfonds finanziert, der nicht Teil des Staatshaushalts ist, sondern ein öffentlicher Fonds, der für Opfer von Straftaten vorgesehen ist[21]. Der Erwerb verstößt daher gegen das polnische Recht. Darüber hinaus erlauben die ursprünglichen Regelungen für diesen Fonds nicht, dass er zur Finanzierung von Tätigkeiten der Sonderdienste verwendet werden kann[22]. Im September 2017 wurde jedoch dem Ausschuss für öffentliche Finanzen des Sejm (die erste Kammer des polnischen Parlaments) von Michał Woś, dem stellvertretenden Justizminister[23] und einem engen Mitarbeiter des Justizministers Zbigniew Ziobro, ein Antrag auf Änderung des Finanzplans des Justizfonds vorgelegt[24]. Die Abgeordneten stimmten dieser Änderung zu. Als später bekannt wurde, dass der Justizfonds zur Finanzierung des Erwerbs von Pegasus für das CBA verwendet wurde, sagten die Abgeordneten, dass „während der Ausschusssitzung kein einziges Wort darüber gesagt wurde“[25]. Es scheint daher, dass sie von der Regierung getäuscht wurden. Obwohl der NIK der Staatsanwaltschaft eine offizielle Mitteilung über einen Verstoß gegen das Gesetz bei der Verwendung von Mitteln aus dem Justizfonds für den Erwerb von Pegasus im Jahr 2017 übermittelt hat, besteht angesichts des derzeitigen institutionellen und politischen Umfelds keine Erwartung, dass die Staatsanwaltschaft in einem solchen Fall tätig werden wird.

24. Woś beantragte auch beim Finanzministerium die Umverteilung der 25 Mio. PLN, die für Pegasus aus dem Justizfonds ausgegeben wurden, auf „andere Tätigkeiten“ zur „Bekämpfung der Auswirkungen von Straftaten“. Der stellvertretende Minister stimmte daraufhin dem Transfer aus dem Justizfonds an das CBA zu. Als Woś jedoch im Januar 2022 danach gefragt wurde, leugnete er zunächst, von Pegasus, geschweige denn von dessen Erwerb durch den Staat, zu wissen, er hat seitdem aber den Erwerb bestätigt. Es ist unklar, wie die laufenden Kosten für den Einsatz von Pegasus finanziert wurden.

25. Es wurde berichtet, dass die NSO Group Pegasus bisher an 14 Länder in Europa verkauft hat. Die NSO Group hat jedoch auch eingeräumt, dass sie die Lizenzen zweier dieser Länder widerrufen hat[26]. In ihrer Aussage vor dem PEGA-Ausschuss erklärte die NSO Group, dass sie „Probleme“ hinsichtlich des Einsatzes von Pegasus nur dann untersucht, wenn sie Informationen von Hinweisgebern oder über die Medien erhält. Erhält die NSO Group Beschwerden, untersucht und überprüft sie diese und kann

---

[21] The Guardian, ‘More Polish opposition figures found to have been targeted by Pegasus spyware’, 17 February 2022; The Guardian, ‘Polish senators draft law to regulate spyware after anti-Pegasus testimony’, 24 January 2022; Bericht der Kommission über die Rechtsstaatlichkeit 2022, Länderkapitel zur Lage der Rechtsstaatlichkeit in Polen, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, S. 26; Gazeta Wyborcza, https://www.rp.pl/polityka/art19250101-gazeta-wyborcza-jak-kupowano-pegasusa-dla-cba, 3 January 2022.

[22] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 January 2022.

[23] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 January 2022; Gazeta Wyborcza, https://wyborcza.pl/7,75398,27966080,jak-ziobro-kupowal-pegasusa-dla-cba.html, 3 January 2022.

[24] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 January 2022.

[25] https://polishnews.co.uk/pegasus-reports-of-surveillance-and-backstage-of-the-purchase-themis-judges-association-on-a-possible-breach-of-the-law-appeal-to-appoint-a-commission-of-inquiry/, 4 January 2022.

[26] Gespräch mit der NSO Group, Informationsreise des Untersuchungsausschusses zur Prüfung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware nach Israel, Juli 2022.

anschließend Pegasus den Akteuren entziehen, die die Software missbraucht haben[27]. Auf der Grundlage der Vielzahl von Medienberichten über den Einsatz von Pegasus in Polen ist es sehr wahrscheinlich, dass Polen aufgrund von Verstößen gegen die Nutzungsbedingungen von NSO eines dieser beiden Länder ist; dies wurde jedoch nicht bestätigt.

26. Seit den ersten Hinweisen auf den Einsatz von Pegasus durch die polnischen Behörden hat der polnische Ombudsmann versucht, sich bei den Behörden zu erkundigen, ob dies der Fall war, und hat sich für eine Verbesserung der Demokratie- und Menschenrechtsgarantien ausgesprochen, um den Missbrauch von Überwachung zu verhindern, unter anderem durch jährliche Berichte an das polnische Parlament. Im Januar 2023 übermittelte der polnische Ombudsmann ein Schreiben an den Innenminister, in dem er erklärte, dass es keine Rechtsgrundlage für den Einsatz von Pegasus oder ähnlicher Spähsoftware in Polen gebe. Dabei berief er sich auf die Rechtsprechung des polnischen Verfassungsgerichtshofs sowie auf die Rechtsprechung des EGMR[28].

RECHTLICHER RAHMEN

27. Im Jahr 2014 führte das Verfassungsgericht eine Überprüfung des Polizeigesetzes von 1990 und anderer bestehender Gesetze zur Überwachung der Bürger durch, die als unvereinbar mit der polnischen Verfassung angesehen wurden[29]. Das Gericht veröffentlichte abschließend ein Urteil mit konkreten Empfehlungen und einem Zeitplan über 18 Monate, innerhalb deren die Gesetzesänderungen umgesetzt werden sollten[30]. Nach den Wahlen 2015 führte die neue Regierung Gesetzesänderungen ein. Das daraus resultierende Gesetz vom 15. Januar 2016 zur Änderung des Polizeigesetzes von 1990 und einiger anderer Gesetze (im Folgenden „das Polizeigesetz von 2016“) hat jedoch keine der vom Verfassungsgerichtshof geforderten Gesetzeslücken behoben[31]. Stattdessen hat das Polizeigesetz von 2016 die ohnehin schon schwachen Bestimmungen, die weder die Rechte der Bürger schützen noch eine angemessene Aufsicht schaffen, weiter abgeschwächt.

28. In ihrer Stellungnahme zum Polizeigesetz von 2016 stellt die Venedig-Kommission fest, dass die im Polizeigesetz festgelegten Verfahrensgarantien und materiellen Bedingungen für die Durchführung der geheimen Überwachung nach wie vor nicht ausreichen, um deren übermäßige Nutzung und ungerechtfertigte Eingriffe in die Privatsphäre des Einzelnen zu verhindern[32]. Darüber hinaus verstößt die fehlende Eindeutigkeit in Bezug auf Kontrolle, Schutz vor Missbrauch und die Kategorien der Personen und Straftaten, die zum Ziel werden könnten, auch gegen Urteile des

[27] Zeugenaussage von Chaim Gelfand, General Counsel und Chief Compliance Officer, NSO, im PEGA-Ausschuss, 21. Juni 2022.
[28] Sitzung des PEGA-Ausschusses, 19. Januar 2023.
[29] Gutachten Nr. 839/2016 zum Gesetz vom 15. Januar 2016 zur Änderung des Polizeigesetzes und bestimmter anderer Gesetze, angenommen von der Venedig-Kommission auf ihrer 107. Plenartagung am 10./11. Juni 2016.
[30] https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani.
[31] Act of 15 January 2016 amending the Police Act and Certain Other Acts at Article 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[32] Gutachten Nr. 839/2016 zum Gesetz vom 15. Januar 2016 zur Änderung des Polizeigesetzes und bestimmter anderer Gesetze, angenommen von der Venedig-Kommission auf ihrer 107. Plenartagung am 10./11. Juni 2016.

EGMR[33]. Insbesondere im Urteil über den Fall *Roman Zakharov*/ *Russland* im Jahr 2015 prüfte der Gerichtshof die Notwendigkeit der Eindeutigkeit in Bezug auf die Verwendung von Spähsoftware. Es wurde festgestellt, dass im Zusammenhang mit der heimlichen Überwachung von Bürgern strenge Kriterien, eine ordnungsgemäße gerichtliche Kontrolle, die sofortige Vernichtung irrelevanter Daten, die gerichtliche Prüfung von Dringlichkeitsverfahren und die Voraussetzung der Benachrichtigung der Opfer erforderlich sind[34]. Darüber hinaus erklärte das Gericht ausdrücklich, dass es „im Widerspruch zur Rechtsstaatlichkeit" stünde, wenn der Ermessensspielraum in Bezug auf heimliche Überwachung ausschließlich in den Zuständigkeitsbereich des Exekutivorgans der Justiz fallen würde[35]. Das Polizeigesetz von 2016, das in Polen in Kraft bleibt, spiegelt dieses Urteil des Gerichts in keiner Weise wider. Tatsächlich stehen seine Bestimmungen in unmittelbarem Widerspruch zu einem Großteil des Urteils.

29. Der EGMR vertrat auch hinsichtlich der Prüfung der Notwendigkeit den eindeutigen Standpunkt, dass die Überwachungstätigkeit von ausreichender Bedeutung sein muss, um einen solchen Eingriff in die Privatsphäre erforderlich zu machen. In seinem Urteil in der Rechtssache *Klass u.a.*/ *Deutschland* aus dem Jahr 1978 wurde dieser Aspekt klar dargelegt und es wurde festgestellt, dass das Gericht unabhängig vom Überwachungssystem davon überzeugt sein muss, dass „hinreichende und wirksame Garantien gegen Missbrauch"[36] vorhanden sind. Die sorgfältig orchestrierte Zerstörung der Gewaltenteilung in Polen zeigt die offensichtliche Missachtung der Gerichte durch die regierende Partei. Trotz allem besteht die von der PiS geführte Regierung darauf, dass die bestehenden Bestimmungen ausreichend sind und streng im Rahmen des Gesetzes operieren[37]. Gleichzeitig hat die Regierung alle Ersuchen um Dialog und Klarstellung über den Einsatz von Überwachungsmechanismen in Polen abgelehnt.

2016 ANTI-TERROR-GESETZ

30. Neben dem Polizeigesetz von 2016 hat der Sejm 2016 auch ein Gesetz zur Überwachung ausländischer Bürger verabschiedet, das er als „Anti-Terror-Gesetz" bezeichnet. Das Gesetz sieht vor, dass nicht-polnische Bürger ohne gerichtliche Zustimmung für einen Zeitraum von drei Monaten – unter anderem durch das Abhören von Telefonen, die Erfassung von Fingerabdrücken, biometrischen Fotos und DNA sowie die Verpflichtung zur Registrierung von Prepaid-Telefonkarten – überwacht werden können, wenn ihre Identität als „zweifelhaft" gilt[38]. Nach Artikel 9 Absatz 8 des Gesetzes ist der Generalstaatsanwalt für die Anordnung der Vernichtung von nicht

[33] Siehe u.a. *Roman Zakharov* v. *Russia* [GC], no. 47143/06, ECtHR, judgment of 4 December 2015; *Klass and others* v. *Germany*, no. 5029/71, ECtHR, judgment of 6 September 1978, paragraph 40; *Prado Bugallo* v. *Spain*, no. 58496/00, ECtHR, judgment of 18 February 2003, paragraph 30; *Liberty and others* v. *United Kingdom*, no. 58243/00, judgment of 1 July 2008, paragraph 62.
[34] *Roman Zakharov* v. *Russia* [GC], no. 47143/06, ECtHR, judgment of 4 December 2015.
[35] *Roman Zakharov* v. *Russia* [GC], no. 47143/06, ECtHR, judgment of 4 December 2015, paragraphs 229 and 230. Siehe auch Gutachten Nr. 839/2016 der Venedig-Kommission vom Juni 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e, S. 11.
[36] *Klass and others* v. *Germany*, 6 September 1978, paragraph 50, Series A no. 28. 40.
[37] Schreiben von Mariusz Kaminski, Minister für Inneres und Verwaltung Polens, an den PEGA-Ausschuss vom 8. September 2022.
[38] Act of 10 June 2016 on Anti-terrorism Operations, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf.

relevantem Unterlagen zuständig. Angesichts der Tatsache, dass der derzeitige Generalstaatsanwalt, Zbigniew Ziobro, auch das Amt des Justizministers innehat, bestehen ernsthafte Bedenken, ob er in der Lage ist, unabhängige und unparteiische Entscheidungen zu treffen, ohne von den politischen Interessen der Regierung, die er vertritt, beeinflusst zu werden[3940].

STRAFPROZESSORDNUNG

31. Im Juli 2015 wurde in Polen das Gesetz zur Änderung der Strafprozessordnung eingeführt, um sicherzustellen, dass illegal erlangte Beweise nicht in Strafverfahren einbezogen werden können. Nach der Machtübernahme der PiS wurde das Gesetz jedoch im März 2016 umgeschrieben, um Artikel 168a aufzunehmen[41]. Dieser Zusatz stellt nun sicher, dass rechtswidrig erlangte Beweismittel bzw. „Früchte des vergifteten Baumes“, wie z. B. Informationen, die durch die Verwendung von Pegasus gewonnen wurden, vor Gericht eingebracht werden können[42]. Es ist jedoch hinzuzufügen, dass der Oberste Gerichtshof Polens in einem Urteil darauf hingewiesen hat, dass dieser Artikel nicht im Widerspruch zu den Bestimmungen der Europäischen Menschenrechtskonvention und der Verfassung Polens angewandt werden kann, die seine wirksame Anwendung in einigen Fällen einschränken[43]. Es wurden auch Urteile erlassen, in denen Artikel 168a teilweise verfassungswidrig befunden wurde[44]. Das Vorhandensein dieser Bestimmung in der Rechtsordnung wirft jedoch Unsicherheit in Bezug auf die Achtung der Grundrechte auf.

TELEKOMMUNIKATIONSGESETZ

32. Nach der Änderung des Telekommunikationsgesetzes von 2004 im Jahr 2016 sieht das polnische Telekommunikationsgesetz dass die Polizei uneingeschränkt und in bestimmten Fällen auch ohne das Zutun von Mitarbeitern der Telekommunikationsgesellschaften auf Telekommunikationsdaten zugreifen kann[45]. Dies kann unter dem vagen Vorwand der „Verhütung oder Aufdeckung von Straftaten“ geschehen. Die Staatsanwaltschaft entscheidet nach Erhalt dieser Daten über das weitere Vorgehen. Dies kann jedoch nicht als Schutzmaßnahme gelten, da die Staatsanwaltschaft durch die Verschmelzung der Rolle des Justizministers mit der des Generalstaatsanwalts nicht als unabhängig von der Exekutive angesehen werden kann[46].

33. Die oben genannte Änderung der Strafprozessordnung zur Verwendung der „Früchten des vergifteten Baumes“ hat erhebliche Auswirkungen auf die Bedeutung der Telekommunikationsbetreiber und der von ihnen gespeicherten Daten. In Polen sind die

[39] Act of 10 June 2016 on Anti-terrorism Operations, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf.
[40] EDRi, https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/, 29 June 2016.
[41] Act of 11 March 2016 amending the Code of Criminal Procedure and Certain Other Acts, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000437/T/D20160437L.pdf.
[42] https://palestra.pl/en/palestra/issue/5-2016/article/article-168a-of-the-polish-criminal-procedure-code-as-a-permission-to-use-illegally-obtained-evidence-in-criminal-proceedings.
[43] Zum Beispiel das Urteil des Obersten Gerichtshofs Polens vom 26. Juni 2019, IV KK 328/18.
[44] Zum Beispiel das Urteil des Obersten Gerichtshofs Polens vom 26. Juni 2019, IV KK 328/18.
[45] Telecommunications Act of 16 July 2004 https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004.
[46] Act of 15 January 2016 amending the Police Act and Certain Other Acts at Article 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.

größten Telekommunikationsanbieter faktisch dazu verpflichtet, ein Team zu haben, dass dazu bestimmt ist, auf Abhöranfragen der Behörden zu antworten. Sie haben jedoch in der Regel nicht viel Einblick in die Abhörtätigkeiten oder in Details von Einzelfällen[47].

DAS GESETZ ZUR UMSETZUNG DER RICHTLINIE ÜBER DEN DATENSCHUTZ BEI DER STRAFVERFOLGUNG

34. Polen hat die Datenschutz-Richtlinie (EU) 2016/680[48], die spezifische Standards für die Erhebung und Verarbeitung personenbezogener Daten durch die Polizei und andere Dienststellen vorsieht, nicht ordnungsgemäß umgesetzt. Die Datenschutz-Richtlinie wurde durch das 2018 verabschiedete Gesetz über den Schutz personenbezogener Daten, die im Zusammenhang mit der Verhütung und Bekämpfung von Straftaten verarbeitet werden, in polnisches Recht umgesetzt. Das Gesetz erweiterte den Anwendungsbereich der in der Richtlinie vorgesehenen Gründe für die Nichtbenachrichtigung von Einzelpersonen über die Verarbeitung ihrer Daten, erheblich und missachtete den in Artikel 17 der Richtlinie vorgesehenen Mechanismus, der Einzelpersonen die Möglichkeit gewährt, ihre Befugnisse über die zuständige Aufsichtsbehörde (in Polen: der Präsident des Amtes für den Schutz personenbezogener Daten) auszuüben. Darüber hinaus sieht das Gesetz einen erheblichen Spielraum für die nationale Sicherheit vor, einschließlich der Erfüllung gesetzlicher Aufgaben durch verschiedene Stellen der Sicherheitskräfte[49].

35. Polen hat auch die Hinweisgeberrichtlinie der EU noch nicht umgesetzt. Es hat die Frist vom Dezember 2021 nicht eingehalten, nachdem der ursprüngliche Gesetzesentwurf gescheitert war. Im April 2022 wurde ein zweiter Entwurf veröffentlicht, aber es wurden keine weiteren Fortschritte erzielt, und die vorgeschlagenen Rechtsvorschriften enthalten deutlich schwächere Bestimmungen. Im Januar 2022 leitete die Kommission ein Vertragsverletzungsverfahren gegen Polen ein, weil die Richtlinie nicht vollständig umgesetzt wurde, und im Februar 2023 beschloss die Kommission, Polen an den EuGH zu verweisen[50].

36. Der Sejm, insbesondere Mitglieder der PiS, erarbeitet derzeit ein Gesetz über die elektronische Kommunikation. Dieses Gesetz würde es den Behörden erleichtern, auf E-Mails und Social-Media-Nachrichten polnischer Bürger zuzugreifen. Anbieter müssten E-Mails und Nachrichten auf ihren Servern speichern, damit die zuständigen

---

[47] https://www.europarl.europa.eu/doceo/document/PEGA-CR-736647_EN.pdf; The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, 17 Februar 2022; https://palestra.pl/en/palestra/issue/5-2016/article/article-168a-of-the-polish-criminal-procedure-code-as-a-permission-to-use-illegally-obtained-evidence-in-criminal-proceedings; https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, S. 16.

[48] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

[49] Adam Bodnar et al., 'How to saddle Pegasus: Observance of civil rights in the activities of security services: Objectives of the reform', September 2019 https://bip.brpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20(OSIOD%C5 %81A%C4 %86 %20PEGAZA).pdf.

[50] https://ec.europa.eu/commission/presscorner/detail/de/ip_23_703.

Gerichte Anordnungen zum Zugriff auf die Daten, IP-Adressen und den Inhalt der Nachrichten erteilen könnten[51].

EX-ANTE-KONTROLLE

37. Obwohl die Überwachung in Polen grundsätzlich einer richterlichen Genehmigung bedarf, dient das Genehmigungsverfahren nicht als Schutz vor Missbrauch, sondern eher als Mittel, um der Überwachung zu politischen Zwecken einen Anschein von Legalität zu verleihen. Es ist nicht ausdrücklich klargestellt worden, ob die Überwachung eines der bisher bekannten Opfer von Pegasus mit richterlicher Genehmigung erfolgte. Anträge auf richterliche Genehmigung einer Überwachungsmaßnahme werden von den Sonderdiensten gestellt[52]. Für die Beurteilung des Antrags stehen den Richtern nur die vom Antragsteller (d. h. den Sonderdiensten) eingereichten Informationen zur Verfügung, und der Staatsanwalt entscheidet, welche Unterlagen vorzulegen sind[53]. Bei den Informationen handelt es sich oft nur um eine Zusammenfassung, die manchmal nicht einmal die grundlegendsten Details über die Zielperson (Name, Beruf, die Straftat, derer sie verdächtigt wird) und die anzuwendenden Überwachungsmethoden enthält.

38. Lehnt ein Richter einen Antrag ab, so ist er dazu verpflichtet, eine solche Entscheidung zu begründen, und es kann Berufung gegen diese Entscheidung eingelegt werden[54]. In dringenden Fällen kann der Staatsanwalt die Anwendung von Abfangmethoden zunächst ohne Zustimmung eines Richters genehmigen, sofern das Gericht anschließend innerhalb von fünf Tagen seine Genehmigung erteilt[55]. Dies ist ein bedeutendes und bewusstes Schlupfloch im polnischen Rechtsrahmen.

39. Anträge auf Genehmigung der Überwachung durch die wichtigsten Agenturen, d. h. das CBA, die Polizei (Policja KGP) und die Nachrichtendienste (Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, Służba Ochrony Państwa, Biuro Nadzoru Wewnętrznego MSWiA und der kürzlich hinzugefügte Inspektorat Służby Więziennej) werden fast ausschließlich dem Bezirksgericht in Warschau (Sad Okręgowy) vorgelegt, wo sich die meisten dieser Agenturen befinden.

40. Jeden Tag werden mehrere Dutzend Überwachungsanträge eingereicht, wodurch das Gericht an seine Kapazitätsgrenzen hinsichtlich der eingehende Prüfung jedes Antrags gerät[56]. Das System, das den Richtern nach dem Zufallsprinzip Fälle zuweist, ist in Polen technisch noch in Betrieb, ist aber nur während der Geschäftszeiten

---

[51] EURACTIV, ‘Polish government working on controversial surveillance bill’, https://www.euractiv.com/section/politics/news/polish-government-working-on-controversial-surveillance-bill/.
[52] Act of 15 January 2016 amending the Police Act and Certain Other Acts at Article 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[53] Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Article 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[54] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef.
[55] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef.
[56] Zeugenaussage von Ewa Wrzosek, länderspezifische Anhörung zu Polen, Sitzung des Untersuchungsausschusses zur Untersuchung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware zu Polen, 15. September 2022.

funktionsfähig. Angesichts der Tatsache, dass die gerichtliche Genehmigung von Überwachungstätigkeiten auf 24-Stunden-Basis erfolgt, bestehen genügend Möglichkeiten für die Umgehung des Systems. Durch die Einreichung eines Antrags am Wochenende oder außerhalb der normalen Geschäftszeiten wird der Fall automatisch dem Richter zugewiesen, der zu diesem Zeitpunkt auf Abruf ist[57]. Die Informationen darüber, wer zu einem bestimmten Zeitpunkt auf Abruf ist, sind den Nachrichtendiensten bekannt, die dann grundsätzlich in der Lage sind, einen „freundlich gesinnten Richter“ auszuwählen, an den sie ihre Überwachungsanfragen stellen können[58]. Darüber hinaus kann die Zufallszuweisung auch von IT-Personal umgangen werden, das Zugang zum System hat und in der Lage ist, „freundlich gesinnten Richtern“ Überwachungsgenehmigungen zuzuweisen[59]. All dies untergräbt die Fähigkeit des Gerichts, eine wirksame gerichtliche Kontrolle durchzuführen.

EX-POST-KONTROLLE

41. Die parlamentarische Kontrolle ist in Polen praktisch nicht vorhanden. Vor 2016 wurde der Parlamentarische Aufsichtsausschuss für die Sonderdienste (KSS) von einem wechselnden Vorsitz, der abwechselnd von der Regierungs- und der Oppositionspartei gestellt wurde, geleitet. Die PiS änderte diese parlamentarische Regel jedoch und setzte die PiS-Mitglieder Waldemar Andzel als ständigen Vorsitzenden und Jarosław Krajewski als stellvertretenden Vorsitzenden dieses Ausschusses ein[60]. Die Regierungsparteien haben die absolute Mehrheit im Ausschuss[61]. Dies macht die Aufsichtsfunktion des Ausschusses bedeutungslos. Darüber hinaus hat die regierungsfreundliche Mehrheit im Sejm die Forderung nach einer parlamentarischen Untersuchung der Vorwürfe des unrechtmäßigen Einsatzes von Spähsoftware abgelehnt[62][63][64][65][66]. Der Senat hingegen, in dem die Regierungsparteien keine Mehrheit haben, setzte Anfang 2022 einen Untersuchungsausschuss ein. Der Ausschuss des Senats verfügt jedoch nicht über die Untersuchungsbefugnisse des Sejm[67], dessen Untersuchungsausschuss Zeugen vorladen und Zeugenaussagen unter Eid anhören kann. Der Ausschuss erfuhr Ablehnung von der Regierungspartei im Sejm,

[57] Zeugenaussage von Ewa Wrzosek, länderspezifische Anhörung zu Polen, Sitzung des Untersuchungsausschusses zur Untersuchung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware zu Polen, 15. September 2022.
[58] Zeugenaussage von Ewa Wrzosek, länderspezifische Anhörung zu Polen, Sitzung des Untersuchungsausschusses zur Untersuchung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware zu Polen, 15. September 2022.
[59] Zeugenaussage von Ewa Wrzosek, länderspezifische Anhörung zu Polen, Sitzung des Untersuchungsausschusses zur Untersuchung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware zu Polen, 15. September 2022.
[60] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS.
[61] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS.
[62] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17 Januar 2022.
[63] European Commission 2022 Rule of Law Report, Country Chapter on the rule of law situation in Poland, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, p. 27.
[64] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 Dezember 2021.
[65] The Guardian, ‘Polish senators draft law to regulate spyware after anti-Pegasus testimony’, 24 Januar 2022.
[66] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 Januar 2022.
[67] European Commission 2022 Rule of Law Report, Country Chapter on the rule of law situation in Poland, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf at pg. 27, fussnote 220.

Regierungsbeamten und Sicherheitsagenturen[68], die sich alle der Zusammenarbeit oder der Durchführung eigener Untersuchungen verweigert haben[69].

42. Auch die Prüfung und Abhilfemaßnahmen anderer unabhängiger Stellen wurden stark geschwächt. Der Oberste Rechnungshof verfügt über wirksame Aufsichtsbefugnisse; seine Mitglieder und Bediensteten sind jedoch ständigen Behinderungen, Belästigungen und Einschüchterungen ausgesetzt, wodurch seine operative Leistungsfähigkeit stark beeinträchtigt wird[70]. Der Sejm hat es bisher versäumt, 10 der 19 Mitglieder des Rates des NIK[71]zu ernennen. Die von den Sonderdiensten unter der Leitung von Minister Kaminski durchgeführte Überprüfung der Ratsmitglieder geht nur sehr langsam vonstatten[72].

43. Wird ein Verstoß gegen das Gesetz vom NIK entdeckt, ist er befugt, dies der Staatsanwaltschaft mitzuteilen[73]. Es obliegt jedoch der Staatsanwaltschaft, auf der Grundlage dieser Mitteilung ein Verfahren einzuleiten. In Situationen, in denen der Staatsanwalt nicht tätig wird, kann der NIK wenig tun. Wenn ein gemeldeter Verstoß die Tätigkeiten der Staatsanwaltschaft selbst betrifft, wird ein Teufelskreis der mangelnden Rechenschaft geschaffen. Darüber hinaus müssen alle Fälle, die der NIK der Staatsanwaltschaft mitgeteilt hat, dem Generalstaatsanwalt gemeldet werden, der auch der Justizminister ist und genau das Ministerium leitet, das die Spähsoftware erworben hat. Der Generalstaatsanwalt ist befugt, Ermittlungen einzustellen oder wieder aufzunehmen, die von der Staatsanwaltschaft eingestellt worden waren. Er kann auch Disziplinarverfahren gegen Staatsanwälte einleiten, die er verdächtigt, falsche Entscheidungen getroffen zu haben.

44. Der derzeitige Ombudsmann Marcin Wiącek wurde 2021 ernannt, als der Sejm und der Senat sich nach einem langen Konflikt auf einen überparteilichen Kompromisskandidaten einigten[74]. In Bezug auf den Fall von Senator Brejza

---

[68] Bloomberg, https://www.bloomberg.com/news/articles/2022-01-03/polish-government-urged-to-probe-spyware-use-as-scandal-grows?leadSource=uverify%20wall#xj4y7vzkg, 3 Januar 2022.
[69] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17 Januar 2022; European Commission 2022 Rule of Law Report, Country Chapter on the rule of law situation in Poland, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, p. 27; AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 Dezember 2021; The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', 24 Januar 2022; Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 Januar 2022.
[70] Reuters, https://www.reuters.com/article/poland-pegasus-idUSL8N2UF596, 4 Februar 2022; Gespräch mit dem Obersten Rechnunghof, Informationsreise des Untersuchungsausschusses zur Untersuchung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware nach Polen, September 2022.
[71] https://www.nik.gov.pl/en/about-us/the-council-of-nik/; Gespräch mit dem Personal des Obersten Rechnungshofs, Informationsreise des Untersuchungsausschusses zur Untersuchung der Verwendung von Pegasus und ähnlicher Überwachungs- und Spähsoftware nach Polen, September 2022.
[72] Gespräch mit dem Personal des Obersten Rechnungshofs, Informationsreise des Untersuchungsausschusses zur Untersuchung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware nach Polen, September 2022.
[73] Act of 23 December 1994 on the Supreme Audit Office, https://www.nik.gov.pl/en/about-us/legal-regulations/act-on-the-supreme-audit-office.html, Article 63.
[74] EURACTIV, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/, 22 Juli 2021.

argumentierte Wiącek, dass der Ombudsmann nicht in die frühen Phasen eines Falls einbezogen werden sollte. Trotzdem haben sowohl die ehemaligen als auch die derzeitigen Ombudspersonen die Situation beobachtet und einen gewissen Druck ausgeübt, was die Notwendigkeit betrifft, ein unabhängiges Aufsichtsgremium einzurichten, das die demokratische Kontrolle über die Tätigkeit der Geheimdienste gewährleistet[75].

BERICHTERSTATTUNG

45. Nach dem Polizeigesetz von 2016 ist die Polizei lediglich verpflichtet, den Gerichten halbjährliche Berichte über die Anzahl der Erhebungen von Telekommunikations-, Post- oder Internetdaten zusammen mit ihrer rechtlichen Begründung (in Bezug auf den Schutz von Menschenleben oder Gesundheit oder zur Unterstützung von Such- und Rettungsmaßnahmen) vorzulegen[76]. Diese Berichte können nur im Nachhinein erstellt werden und werden nicht öffentlich gemacht. Wenn die Vorlage beanstandet wird, legt das Gericht innerhalb von 30 Tagen eine Antwort vor, kann aber nicht die Vernichtung der Daten anordnen, selbst wenn es Unvereinbarkeiten mit dem Gesetz feststellt. Kritisch anzumerken ist, dass diese Kontrollmaßnahmen nur fakultativ und nicht obligatorisch sind.

RECHTSBEHELF

46. Bislang hat die polnische Staatsanwaltschaft nur sehr zögerlich gehandelt, obwohl es zahlreiche Beweise für schwere Straftaten gibt. Es scheint, dass nur der Fall der Staatsanwältin Ewa Wrzosek und der Fall von Krzysztof Brejza von den Gerichten aufgenommen wurden. Wrzosek reichte ihren Fall zunächst bei der Staatsanwaltschaft ein. Als diese sich jedoch offiziell weigerte, den Fall zu übernehmen, konnte sie bei den Gerichten Berufung einlegen. Ende September 2022 wies das Warschauer Bezirksgericht (Mokotów) die Staatsanwaltschaft an, eine Untersuchung einzuleiten. Bislang hat die Staatsanwaltschaft jedoch keine nennenswerten Verfahren eingeleitet, die für den Fortgang der Fälle erforderlich sind, wie etwa die Erfassung von Zeugenaussagen der betroffenen Personen.

47. Es ist von entscheidender Bedeutung, dass Wrzosek nur wegen einer offiziellen Weigerung der Staatsanwaltschaft vor Gericht Berufung einlegen konnte. In vielen anderen Fällen zieht die Staatsanwaltschaft die Ermittlungen in die Länge, um zu vermeiden, jemals eine öffentliche Erklärung abzugeben, in dem Wissen, dass sie somit Teil eines Berufungsverfahrens wird.

48. Von Spähsoftware angegriffene Bürger können einen Zivilprozess vor Gericht bringen, aber die Beweislast dafür, dass sie überwacht wurden, liegt bei ihnen und es ist ohne die Zusammenarbeit der Behörden praktisch unmöglich, den unrechtmäßigen Einsatz von Spähsoftware nachzuweisen. Das Fehlen der Mitteilungspflicht in Polen, wie im Urteil *Klass* dargelegt, bedeutet, dass viele Personen möglicherweise nie erfahren, dass sie

[75] European Parliament. Directorate-General for Parliamentary Research Services, ‘Europe’s PegasusGate: Countering spyware abuse’, study, 6 Juli 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, p. 22.
[76] Act of 15 January 2016 amending the Police Act and Certain Other Acts at Article 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.

angegriffen wurden.

49. Derzeit liegen die Fälle *Pietrzak*/ *Polen* und *Bychawska-Siniarska u. a.*/ *Polen* vor dem EGMR, was den Mangel an Transparenz, Aufsicht, Meldung und Abhilfemaßnahmen in Bezug auf die Überwachung in Polen infrage stellen. Bezeichnenderweise entschied das Gericht, für diese Fälle eine seltene Anhörung durchzuführen, die am 27. September 2022 stattfand. Die Fälle wurden von fünf Bürgern zur Sprache gebracht[77], die im September 2017 bzw. Februar 2018 Beschwerden beim EGMR einreichten. Elf Einrichtungen haben in diesem Fall *Amicus curiae*-Briefe vorgelegt, darunter die Europäische Strafrechtskammer,[78]der polnische Ombudsmann und der Sonderberichterstatter der Vereinten Nationen für die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus[79].

50. Obwohl dieser Beschwerdeweg vor dem EGMR den Bürgern offensteht, ist es fraglich, ob dies angesichts der Dauer des Verfahrens als wirksamer Rechtsbehelf eingestuft wird. Fünf Jahre nach der ursprünglichen Beschwerde gibt es immer noch keine Gerichtsentscheidung in diesem Fall.

51. Auf der Grundlage von Artikel 227 der Verwaltungsprozessordnung wurden Anfang 2017 Beschwerden beim Premierminister und den jeweiligen Leitern der verschiedenen Polizei- und Nachrichtendienste eingereicht. Zu diesen Nachrichtendiensten gehörten das CBA, die Agentur für innere Sicherheit, die nationale Steuerverwaltung, der Militärische Abschirmdienst, die nationale Polizei, die Grenzpolizei und die nationale Gendarmerie. Ihre Beschwerden betrafen die Tatsache, dass die Rechtsvorschriften es den Mitgliedern dieser Polizei- und Nachrichtendienste erlaubten, die Telekommunikation und die digitale Kommunikation der Beschwerde führenden Personen ohne ihr Wissen zu überwachen. Da die Mitglieder der betreffenden Dienste nicht verpflichtet waren, sie über eine mögliche Überwachung zu informieren, konnten die Beschwerde führenden Personen die Rechtmäßigkeit dieser Tätigkeiten, die ihrer Ansicht nach gegen die polnische Verfassung verstießen, folglich nicht durch ein Gericht überprüfen lassen.

52. Zwischen Juni und September 2017 übermittelten die Leiter der oben genannten Polizei- und Nachrichtendienste ihre Antworten auf die Beschwerden der Antragsteller. Unter Berufung auf Artikel 8 (Recht auf Achtung des Privat- und Familienlebens) der Europäischen Menschenrechtskonvention beschwerten sich die Antragsteller, dass die Geheimsysteme zur Überwachung der Telekommunikation, der Post und der digitalen Kommunikation und der Sammlung von Metadaten, die in Anwendung des Polizeigesetzes und des Anti-Terror-Gesetzes eingeführt wurden, ihr Recht auf Achtung ihres Privatlebens beeinträchtigen. Unter Berufung auf Artikel 8 in Verbindung mit

---

[77] Herr Mikołaj Pietrzak, Rechtsanwalt, Dekan der Rechtsanwaltskammer Warschau; Frau Dominika Bychawska-Siniarska, Mitglied und Mitarbeiterin der Helsinki Foundation for Human Rights; Frau Barbara Grabowska-Moroz, Universitätsdozentin und Forscherin sowie externe Expertin der Helsinki-Stiftung für Menschenrechte; Herr Wojciech Klicki und Frau Katarzyna Szymielewicz, Mitglieder der Stiftung Panoptykon mit Sitz in Warschau.

[78] https://www.ecba.org/content/index.php/working-groups/human-rights/857-ecba-hr-office-at-the-echr-hearing-in-the-case-pietrzak-v-poland-and-bychawska-siniarska-and-others-v-poland-hearing-29-09-2022.

[79] https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/SR/AmicusBrief_Poland_SRCT_ECHR.pdf.

Artikel 13 (Recht auf wirksame Beschwerde) machen die Antragsteller geltend, dass sie über keinen wirksamen Rechtsbehelf verfügten, der es ihnen ermöglicht hätte, festzustellen, ob sie selbst Opfer einer heimlichen Überwachung geworden sind, und gegebenenfalls die Rechtmäßigkeit dieser Überwachung durch ein Gericht überprüfen zu lassen.

ÖFFENTLICHE KONTROLLE

53. Unabhängige Medien sind ein weiteres Element der demokratischen Kontrolle und üben eine öffentliche Kontrolle aus. Im Fall des Einsatzes von Spähsoftware hat sich der polnische öffentlich-rechtliche Rundfunk, der weitgehend von den Regierungsparteien kontrolliert wird, jedoch mit der Veröffentlichung von Material, das von den Smartphones mehrerer Zielpersonen, darunter Senator Brejza, stammt, zu einem Komplizen des illegalen Überwachungsskandals gemacht. Die Veröffentlichung von Informationen, die bei einer Überwachungsmaßnahme der Sonderdienste erlangt wurden, stellt an sich bereits eine strafbare Handlung dar. Dennoch wurden weder von der Polizei noch von der Staatsanwaltschaft Maßnahmen ergriffen.

POLITISCHE KONTROLLE

54. Viele Schlüsselpositionen in der gesamten Kontrollkette werden von Mitgliedern oder Loyalisten der Regierungsparteien besetzt. Der Innenminister und Koordinator für Sonderdienste, Mariusz Kamiński, wurde 2015 wegen Machtmissbrauchs zu einer dreijährigen Haftstrafe verurteilt[80]. Unmittelbar nach den Parlamentswahlen 2015 begnadigte ihn Präsident Duda jedoch auf höchst irreguläre Weise, was unter anderem vom Obersten Gerichtshof Polens, dem EuGH, der Venedig-Kommission und dem US-Außenministerium verurteilt wurde. Dies lässt Zweifel an seiner Unabhängigkeit und Neutralität aufkommen. Kaminski hat es abgelehnt, sich mit dem PEGA-Ausschuss zu treffen oder mit ihm zusammenzuarbeiten[81].

55. Das CBA wird vollständig von der Regierungsmehrheit kontrolliert und es fehlt ihm an Unabhängigkeit, trotz seines Titels und seines Auftrags, die gemäß dem Gesetz über das Zentrale Antikorruptionsbüro[82] vom 9. Juni 2006 festgelegt wurden. In dessen Artikel 1 Absatz 1 heißt es, dass das Zentrale Antikorruptionsbüro als besonderer Dienst zur Bekämpfung der Korruption im öffentlichen und wirtschaftlichen Leben, insbesondere in öffentlichen und lokalen Regierungsinstitutionen, sowie zur Bekämpfung von Aktivitäten, die den wirtschaftlichen Interessen des Staates schaden, gegründet wurde[83]. Im jährlichen Bericht über die Rechtsstaatlichkeit 2022 stellt die Kommission fest, dass die Unabhängigkeit der wichtigsten Organe zur Korruptionsbekämpfung nach wie vor ein Thema ist, wobei insbesondere die Unterordnung des Zentralen Antikorruptionsbüros unter die Exekutive und die Tatsache, dass der Justizminister

[80] *Reuters*, https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117, 17. November 2015.
[81] EU Observer, https://euobserver.com/rule-of-law/156063, 15. September 2022.
[82] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf.
[83] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf, Art. 1.1.

zugleich der Generalstaatsanwalt ist, zu berücksichtigen sind[84].

56. Die Bemühungen der Regierung, die Kontrolle über die Justiz zu erlangen, wurden umfassend dokumentiert und durch eine Vielzahl von Instanzen, darunter die Kommission, den EuGH und den EGMR, bestätigt.

57. Es wurde nicht nur der rechtliche und institutionelle Kontext geschaffen, um eine nahezu unbegrenzte Überwachung mit Spähsoftware zu ermöglichen, sondern praktisch alle Teile des Prozesses werden auch von den Regierungsparteien fest kontrolliert. Infolgedessen haben Sicherheitsvorkehrungen, die theoretisch existieren, in der Praxis keine oder wenig Bedeutung.

DIE ZIELE

58. Die ersten dokumentierten Fälle des Einsatzes von Pegasus in Polen stammen aus dem Jahr 2018. Einer davon betraf den ehemaligen stellvertretenden Finanzminister Paweł Tamborski, dessen Telefon im Februar 2018 mit Pegasus gehackt wurde, was Amnesty International und Wyborcza im Juli 2022 aufdeckten. Am selben Tag verhaftete das CBA ihn sowie fünf ehemalige Beamte des Ministeriums und Marktanalysten, denen vorgeworfen wurde, den Marktwert des Chemikalienunternehmens CIECH im Austausch gegen Bestechungsgelder unterbewertet zu haben. Das Gericht stimmte der Festnahme nicht zu und ordnete ihre Freilassung an. Der Geschäftsführer und Eigentümer der PR-Agentur Cross Media, Andrzej Długosz, wurde ebenfalls angegriffen und zwischen März 2018 und November 2019 mindestens 61 Mal gehackt. In der Folge forderte der Ombudsmann mehr Informationen von den Behörden an, doch die Bemühungen waren vergeblich. Zu dieser Zeit leugnete die Regierung, die Spähsoftware erworben zu haben.

59. Im Rahmen von Untersuchungen von Associated Press und den Forschern von Citizen Lab an der Universität von Toronto wurde aufgedeckt, dass 2019 drei weitere Personen in Polen von Pegasus ins Visier genommen wurden[85]. Bei den Zielpersonen handelte es sich um den oppositionellen Senator Krzysztof Brejza, den Rechtsanwalt Roman Giertych und die Staatsanwältin Ewa Wrzosek. Zwar haben einige Mitglieder der Regierungsmehrheit den Erwerb der Software von der NSO Group bestätigt, doch die Regierung hat nicht offiziell bestätigt, dass bestimmte Personen damit ausgespäht wurden. Keine der drei Zielpersonen wurde formell eines Verbrechens angeklagt, noch wurden sie zur Befragung vorgeladen oder ein Antrag auf Aufhebung der Immunität der Zielpersonen, die politische Ämter im Zusammenhang mit diesem Fall bekleiden, gestellt.

60. Citizen Lab hatte Ende 2017 eine Reihe von Infizierungen mit Spähsoftware in Polen festgestellt, war jedoch zu diesem Zeitpunkt nicht in der Lage, die Zielpersonen zu identifizieren[86].

---

[84] Berichtder Kommission über die Rechtsstaatlichkeit 2022, Länderkapitel zur Lage der Rechtsstaatlichkeit in Polen, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, S. 1.
[85] The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, *17 Februar 2022.*
[86] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. Dezember 2021.

61. Der Einsatz von Spähsoftware und die Versuche, Bürger zu kontrollieren, müssen in enger Verbindung mit dem Wahlsystem betrachtet werden. Mehrere Ziele von Pegasus waren in gewisser Weise mit Wahlen verbunden: Senator Krzysztof Brejza (Wahlkampfleiter für die größte Oppositionspartei), Roman Giertych (Rechtsanwalt des Oppositionsführers und ehemaligen Präsidenten des Europäischen Rates, Donald Tusk), Ewa Wrzosek (die Staatsanwältin, die die Briefwahl bei den Präsidentschaftswahlen untersuchte), der Oberste Rechnungshof (NIK; er veröffentlichte Berichte über die Briefwahl für die Präsidentschaftswahlen) und Michael Kolodziejczak (Gründer einer Bauernpartei, die im selben Wahlkampf antritt wie die Regierungsparteien).

62. Gleichzeitig wurde die Unabhängigkeit der Nationalen Wahlkommission dadurch in Frage gestellt, dass sie aus Richtern besteht, die vom Parlament und von Gerichten ausgewählt wurden, die die Regierungspartei unter ihre Kontrolle gebracht hat. Darüber hinaus wurde das für die Registrierung neuer Parteien zuständige Bezirksgericht in Warschau mit[87] regierungstreuen „Neurichtern“ besetzt, deren Unabhängigkeit in Frage gestellt werden könnte.

KRZYSZTOF BREJZA

63. Senator Krzysztof Brejza war während der europäischen und der nationalen Wahlen als Wahlkampfleiter der Oppositionspartei „Bürgerplattform“ tätig, als er Opfer eines Hackerangriffs mit Spähsoftware wurde[88]. Es gab 33 Angriffe auf Brejzas Telefon in der Zeit, in der er die Kampagne der Bürgerplattform 2019 leitete. Die Angriffe begannen am 26. April 2019 und dauerten bis zum 23. Oktober 2019, nur wenige Tage nach dem Ende des Wahlzyklus, an[89].

64. Als direkte Folge des Hackerangriffs auf Brejzas Telefon wurden mutmaßlich Textnachrichten während der Wahlen 2019 in einer mutmaßlich orchestrierten Verleumdungskampagne gestohlen[90], verändert und anschließend im staatlich kontrollierten Polnischen Fernsehen (TVP) veröffentlicht[91]. Dies hat Senator Brejza dazu veranlasst, die Legitimität der Wahl 2019 in Frage zu stellen, die die regierende PiS-Partei knapp gewann[92].

65. Obwohl die PiS-Regierung zugibt, Pegasus erworben zu haben, leugnet sie vehement die Vorwürfe, dass die Software für politische Zwecke eingesetzt wurde[93]. Kaczynski

[87] Act of 27 June 1997 on Political Parties, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970980604/U/D19970604Lj.pdf, Article 11.
[88] Haaretz, https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000, 5. April 2022.
[89] The Guardian, ‘More Polish opposition figures found to have been targeted by Pegasus spyware’, 17 February 2022.
[90] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 December 2021.
[91] Commission 2022 Rule of Law Report, Country Chapter on the rule of law situation in Poland, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, pp. 20-23; AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 December 2021.
[92] Financieele Dagblad, https://fd.nl/politiek/1426857/liberalen-europarlement-eisen-onderzoek-naar-spionagesoftware, 12 January 2022.
[93] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 January 2022.

hat weder bestätigt noch bestritten, Brejza angegriffen zu haben, behauptete aber, dass der Senator mit „mutmaßlichen Straftaten“ in Verbindung steht, was Brejza stark leugnet[94]. Brejza wurde nie eines Verbrechens angeklagt, noch wurde er zur Befragung vorgeladen. Dies deutet darauf hin, dass der Einsatz der Spähsoftware keinem investigativen Zweck diente. Durch die Andeutung, Brejza stehe mit kriminellen Aktivitäten in Verbindung, versuchte die Regierung, den Einsatz von Spähsoftware formal zu legitimieren, indem sie Umstände schuf, unter denen die polnische Regierung die Pegasus-Spionagesoftware aus einem der Gründe einsetzen konnte, die die NSO Group als „berechtigte Gründe“ ansieht, um ihre Software an eine Regierung zu verkaufen, nämlich die Untersuchung schwerwiegender krimineller Aktivitäten[95].

66. Wochenlang war Senator Brejza das Ziel einer Verleumdungskampagne, die sich auf Material stützte, das durch den Einsatz von Spähsoftware gewonnen wurde. Die Tatsache, dass dieses Material über das öffentliche Fernsehen veröffentlicht wurde, ist besonders alarmierend. Es kann keine Erklärung dafür geben, wie ein öffentlich-rechtlicher Sender Zugang zu solchen Materialien erhält. Sollte es sich – wie die Regierung zu behaupten scheint – bei dem Hacking von Senator Brejza mit der Spähsoftware „Pegasus“ tatsächlich um eine Angelegenheit der nationalen Sicherheit gehandelt haben, würde die Weitergabe von Material, das im Rahmen einer geheimen Sicherheitsoperation erlangt wurde, ein sehr schweres Verbrechen darstellen. Die Tatsache, dass auch der öffentlich-rechtliche Rundfunk von der Regierungspartei beherrscht wird, lässt eher eine von den Regierungsparteien orchestrierte Verleumdungskampagne vermuten.

67. Zu dieser Zeit wurde jedoch eine strafrechtliche Untersuchung gegen den Vater von Senator Brejza, Ryszard Brejza, eingeleitet. Während seiner Amtszeit als Bürgermeister von Inowroclaw, einer Stadt in Zentralpolen, wurde Brejza Sr wegen angeblicher falscher Verwaltung öffentlicher Gelder und Nichterfüllung seiner Aufgaben zur Befragung vorgeladen[96]. Diese Vernehmung ereignete sich unmittelbar, nachdem Brejza Jr ein Gerichtsverfahren gegen Kaczynski wegen Verleumdung eingeleitet hatte. Sowohl Krzysztof als auch Ryszard Brejza machten geltend, dass die Anklagen gegen Brejza Sr eine Vergeltungsmaßnahme für die Einreichung der Klage war.

68. Ryszard Brejza selbst erhielt zwischen Juli und August 2019 10 Textnachrichten, die das Sicherheitslabor von Amnesty International als verdächtig einstufte und die den typischen Markenzeichen von Pegasus entsprachen[97]. Darüber hinaus erhielt Senator Brejzas ehemalige Assistentin Magdalena Losko im April 2019 vier verdächtige Textnachrichten, die laut forensischen Prüfern von Amnesty International technisch mit der Spähsoftware „Pegasus“ der NSO Group übereinstimmten[98].

---

[94] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 January 2022.
[95] BBC, https://www.bbc.com/news/technology-57881364, 19 July 2021.
[96] AP, https://apnews.com/article/technology-business-software-hacking-spyware-8cc528ba7d46a61b378adf1ede9dd00f, 10 January 2022.
[97] The Guardian, ‘More Polish opposition figures found to have been targeted by Pegasus spyware’, 17 February 2022; Le Monde, https://www.lemonde.fr/pixels/article/2022/07/18/affaire-pegasus-un-an-apres-le-crepuscule-de-nso-group_6135168_4408996.html, 18 July 2022.
[98] The Guardian, ‘More Polish opposition figures found to have been targeted by Pegasus spyware’, 17 February 2022.

ROMAN GIERTYCH

69. Roman Giertych wurde in den letzten Wochen vor den Parlamentswahlen 2019 mit der Spähsoftware „Pegasus“ ausgespäht. Zwischen September und Dezember 2019 wurde Giertych ganze 18 Mal gehackt. Die meisten Angriffe fanden kurz vor dem Wahltermin am 13. Oktober 2019 statt. Zu dieser Zeit war er als Anwalt des Vorsitzenden der Oppositionspartei „Bürgerplattform“ und ehemaligen Premierministers Donald Tusk tätig. In dieser Zeit vertrat Giertych auch Radek Sikorski, den ehemaligen Außenminister und derzeitiges Mitglied des Europäischen Parlaments für die Europäische Volkspartei (PPE). Sikorski untersuchte die Verwicklung Kaczynskis und seiner Verbündeten in illegale Abhörmaßnahmen, bei denen Gespräche des Ministers aufgenommen und veröffentlicht wurden[99].

70. Wie im Fall von Senator Brejza hat die Regierung weder bestätigt noch dementiert, dass sie für diese Angriffe verantwortlich ist. Associated Press berichtete, dass ein Staatsanwalt einen Antrag auf Verhaftung Giertychs im Zusammenhang mit angeblichen Ermittlungen wegen Finanzdelikten gestellt habe, und zwar nur wenige Stunden, bevor der Sprecher für Fragen der Staatssicherheit, Stanislaw Zaryn, auf Fragen von AP bezüglich des Hackerangriffs auf Giertychs Telefon reagierte. Giertych bestreitet diese Anschuldigungen vehement. Zaryn lehnte es ab, sich zu einem möglichen Zusammenhang zwischen diesen Vorfällen zu äußern. Bei einem ähnlichen Vorfall wurde im Jahr 2020 Giertychs Wohnung von CBA-Beamten gestürmt und durchsucht[100].

71. In dieser Zeit im Jahr 2019 vertrat Giertych auch den österreichische Entwickler Gerald Birgfellner. Birgfellner war an einem Bauprojekt für den PiS-Vorsitzenden Jarosław Kaczynski beteiligt, mit dem er familiäre Bindungen hat, als der Deal abgebrochen wurde. Nach der Veröffentlichung von aufgezeichneten Gesprächen zwischen den beiden brach ein politischer Skandal für Kaczynski aus, der das Projekt dann absagte. Birgfellner behauptet, dass er für seine Dienstleistungen nie bezahlt worden sei und deshalb Giertych engagierte[101]. Justizminister und Generalstaatsanwalt Zbigniew Ziobro erklärte 2021 ebenfalls, er wolle gegen Giertych „mit dem Verdacht der Begehung von Straftaten“ Anklage erheben[102].

EWA WRZOSEK

72. Die Staatsanwältin Ewa Wrzosek wurde zwischen dem 24. Juni und dem 19. August 2020 gleich sechs Mal Opfer eines Hackerangriffs mit der Spionagesoftware „Pegasus“[103]. Wrzosek ist Mitglied der Lex Super Omnia, einer Gruppe von

---

[99] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.
[100] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.
[101] AP, https://apnews.com/article/elections-international-news-jaroslaw-kaczynski-european-parliament-poland-bed5ffc814e649f4bb4d10f82628b4c2, 16 February 2019; TVP World, https://tvpworld.com/41262080/ruling-party-leader-im-no-dictator, 11 February 2019.
[102] TVP Info, https://www.tvp.info/57607147/zaryn-ws-senatora-brejzy-falszywe-sa-sugestie-ze-sluzby-nielegalnie-wykorzystuja-kontrole-operacyjna-do-gry-politycznej, 23 December 2021.
[103] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.

Staatsanwälten, die sich für die Unabhängigkeit der Staatsanwaltschaft einsetzen. Sie leitete zu dieser Zeit Untersuchungen zur Durchführung von Präsidentschaftswahlen 2020 inmitten der weltweiten COVID-19-Pandemie. Dieser Fall wurde ihr entzogen und anschließend fallen gelassen. Es liegt im Zuständigkeitsbereich des Generalstaatsanwalts Zbigniew Ziobro und seiner „rechen Hand“, Staatsanwalt Bogdan Święczkowski, zu entscheiden, bestimmte Fälle nicht strafrechtlich zu verfolgen oder nachgeordnete Staatsanwälte aus bestimmten Fällen zu entfernen[104]. Anschließend wurde Staatsanwältin Wrzosek mit nur 48-stündiger Vorankündigung an eine andere Staatsanwaltschaft in einer mehrere Stunden von ihrem Wohnsitz entfernten Stadt transferiert. Als sie nach Warschau zurückkehrte, wurde sie mit der Spähsoftware Pegasus angegriffen. Die polnischen Behörden waren nicht dazu bereit, die Verantwortung für den Angriff zu übernehmen bzw. diese zu leugnen[105][106].

73. Wrzosek hat auch eine Beschwerde wegen des „Pegasus“-Angriffs ihres Mobiltelefons eingereicht. Das Gericht ordnete ein Gutachten von Citizen Lab zum „Pegasus“-Angriff an und Wrzosek selbst beantragte, ihr Telefon von den Experten von Citizen Lab überprüfen zu lassen. Die Staatsanwaltschaft lehnte diesen Antrag jedoch ab und wählte einen anderen Experten aus, der keine Infektion mit Pegasus feststellen konnte. Darüber hinaus forderte die Staatsanwaltschaft den Telekommunikationsbetreiber auf, alle Metadaten zu Wrzosek für einen Zeitraum vorzulegen, der für die gerichtlichen Ermittlungen unerheblich war. Wrzosek ist der Ansicht, dass sie immer noch überwacht wird und dass das Verfahren der Staatsanwaltschaft darauf abzielt, zusätzliche Beweise zu liefern, die in anderen Fällen gegen sie verwendet werden könnten[107].

74. Wie Wrzosek in der Sitzung des PEGA-Ausschusses vom 19. Januar 2023 hervorgehoben hat, wird sie derzeit von der Staatsanwaltschaft angeklagt, Informationen über einen Fall, der nicht mit Pegasus zu tun hat, offengelegt zu haben und an politischen Aktivitäten beteiligt zu sein. Wrzosek ist nicht in der Lage, ihre Rechtsverteidigung aufzubauen, da die Staatsanwaltschaft den Zugang zu Dokumenten verweigert[108]. Dies scheint eine klare Verletzung des Rechts auf ein faires Verfahren zu sein und erweckt den Eindruck, dass der einzige Zweck des Falles darin besteht, Wrzosek zu diskreditieren.

ANDERE MÖGLICHE ZIELE

OBERSTER RECHNUNGSHOF

75. Der Oberste Rechnungshof (NIK) ist mit der Überwachung der öffentlichen Ausgaben und der Verwaltung der öffentlicher Dienste beauftragt und legte die Rechnungen für den „Kauf von Spezialtechnologien zur Aufdeckung und Verhütung von Straftaten“ in Höhe von insgesamt 25 Mio. PLN offen. Zwar war er kein Ziel von Pegasus, wurde aber von den polnischen Behörden angegriffen und belästigt. Der Zeitpunkt der

[104] European Commission 2022 Rule of Law Report, Country Chapter on the rule of law situation in Poland, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, p. 16.
[105] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw--8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.
[106] The Guardian, https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony, 24 Januar 2022.
[107] Sitzung des PEGA-Ausschusses, 19. Januar 2023.
[108] Sitzung des PEGA-Ausschusses, 19. Januar 2023.

Angriffe ist angesichts der Art der Ermittlungen, die der NIK durchführte, besonders relevant. Der Sprecher des NIK bestätigte, dass er die Absage der Präsidentschaftswahlen im Jahr 2020 untersuchte. Die Untersuchung ergab, dass der Premierminister, Mitglieder seiner Regierung und ein Fonds des Justizministeriums Meldungen über Verbrechen erhalten hatten. Dies scheint den Verdacht zu verstärken, dass Pegasus in Polen überwiegend für politische Zwecke verwendet wurde[109].

MITGLIEDER DER PIS-PARTEI

76. Es gibt die Vermutung, dass Pegasus für das „präventive Abhören" von Anführern und Organisatoren von Straßenprotesten eingesetzt wurde, die zum Protest gegen die von der PiS-Partei durchgeführten Reformen des Verfassungsgerichts stattfanden. Es wurden jedoch womöglich nicht nur Gegner der Regierungspartei mithilfe der Spähsoftware „Pegasus" ausgespäht. Wyborcza zitiert Quellen, derer zufolge Adam Hofman, ehemaliger Sprecher der PiS-Partei, 2018 ausgespäht wurde - nach dem Erwerb der Spähsoftware gehörte er zu den ersten Zielpersonen, die damit ausgespäht wurden. Hofman gründete nach seinem Ausschluss aus der PiS-Partei das PR-Unternehmen R4S[110][111]. Berichten zufolge verärgerte diese Aktion die Regierungspartei und machte Hofman zur Zielscheibe von Überwachungsmaßnahmen. Ihm zufolge wurden die über ihn gesammelten Informationen anschließend in einer Verleumdungskampagne gegen ihn verwendet.

77. Darüber hinaus wurden laut Wiadomości der ehemalige Abgeordnete Mariusz Antoni Kaminski und der ehemalige Minister des Staatsfinanzministeriums, Dawid Jackiewicz, mutmaßlich von der Regierung mit Pegasus angegriffen[112]. Mariusz A. Kaminski wurde aus der PiS-Partei ausgeschlossen, nachdem er gleichzeitig mit Hofman in einen Skandal verwickelt war. Jackiewicz hingegen bleibt trotz seines plötzlichen Rücktritts von seiner Ministerrolle ein Mitglied der Regierungspartei[113].

78. Eine ähnliche Verleumdungskampagne wurde auch gegen den ehemaligen Präsidenten des Arbeitgeberverbands der Republik Polen, Andrzej Malinowski, von der Regierungspartei im Februar 2018 durchgeführt. Er sagte vor Sondersitzung eines Senatsausschusses im April 2022 bezüglich des Pegasus-Hackerangriffs auf sein Telefon zur Gewinnung von Informationen für diese Verleumdungskampagne als Zeuge aus[114]. Er beschrieb, dass WhatsApp- und SMS-Nachrichten von Pegasus abgerufen und strategisch verwendet wurden, um im Internet Hass gegen ihn zu verbreiten. Dieser Angriff sei eine Vergeltungsmaßnahme gegen ihn aufgrund seiner Uneinigkeit mit der Regierungspartei und seiner Forderung einer alternativen Wirtschaftspolitik gewesen.

---

[109] Notes from Poland, https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/, 7 February 2022.
[110] https://wyborcza.pl/7,173236,28015977,polish-state-surveilled-nearly-50-targets-with-pegasus-spyware.html?disableRedirects=true.
[111] Rzeczpospolita, https://www.rp.pl/polityka/art4805251-hofman-usuniety-z-pis-decyzja-w-sprawie-hofmana, 11 Oktober 2014.
[112] https://wiadomosci.onet.pl/kraj/pegasus-oto-kolejne-osoby-ktore-mialy-byc-inwigilowane-przez-sluzby-pis/yvt6tym
[113] https://nextvame.com/dawid-jackiewicz-is-back-jaroslaw-kaczynski-confirms-the-reports/.
[114] https://www.senat.gov.pl/prace/komisje-senackie/przebieg,9668,1.html.

79. Der Missbrauch der Pegasus-Spähsoftware in Polen muss im vollen Kontext der Krise der Rechtsstaatlichkeit des Landes gesehen werden, die im Jahr 2015 begann, als die Regierung unter Führung der PiS mit dem Abbau des Justizsystems begann und seitdem systematisch die wichtigsten Institutionen des Landes übernommen hat und alle strategischen Ämter mit Loyalisten besetzt. Die Regierungspartei stellte gezielt und methodisch die rechtlichen, institutionellen und politischen Bausteine dieses Systems zusammen, um einen kohärenten und hochwirksamen Rahmen zu schaffen, in dem der Einsatz von Pegasus ein integraler und essenzieller Bestandteil eines Systems zur Überwachung der Opposition und der Regierungskritiker ist. Das System wurde aufgebaut, um die Regierungsmehrheit und die Regierung an der Macht zu halten.

80. Der Spielraum für Überwachungstätigkeiten in Polen wurde in den letzten Jahren erheblich ausgedehnt, wodurch Sicherheitsvorkehrungen und Aufsichtsvorschriften geschwächt oder aufgehoben wurden. Im Zuge systematischer und gezielter Gesetzesänderungen durch die Regierungsmehrheit wurden die Rechte der Opfer minimiert und Rechtsbehelfe und -mittel in der Praxis bedeutungslos gemacht. Wirksame Ex-ante- und Ex-post-Prüfungen sowie eine unabhängige Kontrolle wurden de facto beseitigt. Mitglieder der polnischen Regierung und Loyalisten kontrollieren die wichtigsten Ämter innerhalb des Systems direkt oder indirekt. Die mit Spähsoftware gewonnenen Informationen werden in Verleumdungskampagnen durch die staatlich kontrollierten staatlichen Medien gegen Regierungskritiker und die Opposition verwendet. Aufgrund der Tatsache, dass die polnische Regierung die Gesetze systematisch und gezielt nach innerstaatlichem Recht erweitert hat, verstößt die Rechtsgrundlage für die Überwachung weiterhin gegen das EU-Recht, das Urteil des polnischen Verfassungsgerichts von 2014 und die Grundrechte der polnischen Bürger. Auf diese Weise wurde die unrechtmäßige Überwachung, die eindeutig gegen europäisches und nationales Recht verstößt, im Wesentlichen legalisiert.

I. B. Ungarn

81. Ungarn war eines der ersten Länder, das in den europäischen Skandal um die Spähsoftware „Pegasus“ verwickelt war. Im Jahr 2021 enthüllte das Pegasus-Projekt, was auch von Amnesty International bestätigt wurde[115], dass mehr als 300 Ungarn möglicherweise Opfer von missbräuchlichen Einsätzen von Pegasus geworden sind, darunter politische Aktivisten, Investigativjournalisten, Anwälte, Unternehmer, ein Oppositionspolitiker und ein ehemaliger Regierungsminister.

82. Im Februar 2023 reiste eine Delegation des PEGA-Ausschusses nach Ungarn. Sie gelangte zu dem Schluss, dass alle Anzeichen dafür sprechen, dass Spähsoftware in Ungarn grob missbraucht wurde, und die Erklärung der Behörden unter Berufung auf die nationale Sicherheit wurde als sehr wenig überzeugend erachtet. Es liegen starke Anzeichen dafür vor, dass das Ausspähen von Personen dem Ziel diente, noch größere politische und finanzielle Kontrolle über die Öffentlichkeit und den Medienmarkt zu

[115] Euractiv, ‘Hungary employed Pegasus spyware in hundreds of cases, says government agency’, *1 February 2022.*

erlangen.

83. Der Ausschuss war davon überzeugt, dass die Rechtsstaatlichkeit und die demokratischen Grundstandards in Ungarn ernsthaft verletzt wurden und dass die Lage des Landes im EU-weiten Vergleich besonders schlimm ist. Aufgrund jahrelanger demokratischer Rückschläge scheinen die staatlichen Institutionen nicht darauf ausgerichtet zu sein, den Bürgern zu dienen und ihre Rechte und Freiheiten zu schützen, sondern vielmehr darauf, die politischen Ziele der Regierung zu verfolgen. Der Ausschuss forderte die Behörden auf, eine aussagekräftige Untersuchung missbräuchlicher Praktiken zu ermöglichen.

ERWERB VON PEGASUS

84. Im Jahr 2017 stimmte der Nationale Sicherheitsausschuss des ungarischen Parlaments dafür, den Nachrichtendiensten des Landes den Erwerb bestimmter Ausrüstungsmaterialien nach dem regulären Vergabeverfahren zu gestatten. Auf Antrag des Sonderdienstes für nationale Sicherheit (Nemzetbiztonsági Szakszolgálat, NBSZ) unterstützte das ungarische Parlament den Erwerb von hochentwickelter Spähsoftware[116]. Das Verfahren war jedoch geheim, und die Genehmigungsanträge enthielten nicht die spezifische Marke und Art der Technologie[117].

85. Das ungarische Innenministerium erwarb Die Spähsoftware „Pegasus“ im Jahr 2017 für 6 Millionen Euro indirekt über Communication Technologies Ltd von der NSO Group in Luxemburg, kurz nachdem Orbán sich mit dem polnischen Premierminister Mateusz Morawiecki und dem ehemaligen israelischen Premierminister Benjamin Netanjahu getroffen hatte[118][119]. Das ungarische Innenministerium räumte dies erst im November 2021 ein, als der Vorsitzende des parlamentarischen Ausschusses für Verteidigung und Strafverfolgung, Lajos Kósa, den Erwerb von Pegasus durch die Fidesz-Regierung bestätigte[120]. Kósa beharrte jedoch weiterhin darauf, dass die Spähsoftware nie gegen ungarische Bürger eingesetzt wurde[121].

86. Die ungarische Behörde für Datenschutz und Informationsfreiheit (NAIH) erkundigte sich nach dem Vergabeverfahren für den Erwerb der Spähsoftware und erhielt Zugang zu dem geheimen Vertrag mit NSO. Während der Informationsreise von PEGA nach Budapest im Februar 2023 erklärte der Präsident der NAIH, Attila Péterfalvi, zunächst, dass es nicht wahr sei, dass die Bereitstellung von Pegasus an die ungarischen Behörden eingestellt worden sei, was bedeuten würde, dass Ungarn nicht zu den beiden EU-

[116] Study – ‘The use of Pegasus and equivalent spyware – The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware, European Parliament, Directorate-General for Internal Policies, Policy Department C – Citizens’ Rights and Constitutional Affairs, 5 December 2022, available at:
https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.
Direkt36, The inside story of how Pegasus was brought to Hungary, https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/.
[117] Informationsreise des PEGA-Ausschusses nach Ungarn, Treffen mit Mitgliedern des Nationalen Sicherheitsausschusses des ungarischen Parlaments, 20./21. Februar 2023.
[118] Financieele Dagblad, De wereld deze week:Het beste uit de internationale pers. 7 January, 2022.
[119] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 Juli 2021.
[120] DW, Hungary admits to using NSO Group’s Pegasus spyware’, 4 November 2021.
[121] DW, Hungary admits to using NSO Group’s Pegasus spyware’, 4 November 2021.

Mitgliedstaaten gehört, die von der Liste der 14 Mitgliedstaaten, an die NSO „Pegasus“ liefert, entfernt wurden. Péterfalvi zog später seine Erklärung zurück und behauptete, er habe keine Informationen darüber, ob NSO den Einsatz von Pegasus in Ungarn eingestellt habe oder nicht.

RECHTLICHER RAHMEN

87. In Ungarn ist der Rahmen für das rechtmäßige Abfangen von Kommunikationen im Rahmen einer strafrechtlichen Ermittlung im Polizeigesetz festgelegt. Nach dem Polizeigesetz kann die Überwachung von Privatpersonen in einer strafrechtlichen Untersuchung nur mit richterlicher Genehmigung durchgeführt werden. In Angelegenheiten im Zusammenhang mit Terrorismus bezieht sich das Polizeigesetz jedoch auf die im Gesetz zur nationalen Sicherheit erwähnte Untersuchungsüberwachung[122]. Nach dieser Bestimmung muss keine richterliche Genehmigung beantragt werden, um den Einsatz von Überwachungstechniken zu genehmigen, da der Justizminister für die Erteilung der Genehmigung zuständig ist[123]. Anträge auf Genehmigung der Überwachung erwähnen nicht die Art der Technologie, die verwendet werden soll[124].

88. Gemäß dem Gesetz CXXV von 1995 wird das nationale Sicherheitsinteresse als Sicherung der Souveränität und des Schutzes der rechtmäßigen Ordnung Ungarns in dem Rahmen dieses Gesetzes definiert, was eine ziemlich weit gefasste Definition ist.

89. In einem wegweisenden Fall (*Szabó und Vissy* / *Ungarn*[125]) stellte der Europäische Gerichtshof für Menschenrechte (EGMR) fest, dass das Gesetz über die nationale Sicherheit keine hinreichend präzisen, wirksamen und umfassenden Garantien für die Anordnung, Vollstreckung und mögliche Abhilfe von Überwachungsmaßnahmen vorsieht. Das Gesetz über die nationale Sicherheit enthält nicht nur keine Verpflichtung zur Benachrichtigung der überwachten Personen, sondern schreibt ausdrücklich vor, dass die Zielpersonen von der autorisierenden Partei nicht darüber informiert werden dürfen, dass sie ausspioniert werden[126]. Die Verpflichtung zur Benachrichtigung der Zielpersonen wurde im Fall von *Klass u. a./Deutschland*[127] vor dem EGMR eindeutig festgestellt. Darüber hinaus gibt es weder wirksame Rechtsbehelfe und Rechtsmittel im Falle eines Missbrauchs, noch eine ordnungsgemäße Kontrolle. Die ungarische Regierung hat es bisher versäumt, beide Urteile umzusetzen.

EX-ANTE-KONTROLLE

90. Gemäß dem Gesetz zur nationalen Sicherheit ist die Überwachung durch den Sonderdienst für nationale Sicherheit (SNSS) unter Verwendung von Spähsoftware in

---

[122] European Union Agency for Fundamental Rights (FRA), ‘National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary’, 26 September 2014.
[123] FRA, ‘National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary’, legal update, 23 October 2017.
[124] Informationsreise des PEGA-Ausschusses nach Ungarn, 20./21. Februar 2023.
[125] Szabó and Vissy v. Hungary, application no 37138/14, judgment of 12 January 2016, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}.
[126] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf.
[127] Klass and others v. Germany, 6 September 1978, paragraph 50, Series A, no. 28.

den meisten Fällen von der Genehmigung des Justizministers und in einigen besonderen Fällen von dem vom Präsidenten des Landgerichts Budapest-Hauptstadt benannten Richter abhängig[128][129]. Gegen diese Entscheidungen kann kein Rechtsbehelf eingelegt werden, und es findet praktisch keine Beaufsichtigung des Prozesses statt[130][131].

91. Die derzeitige Justizministerin Judit Varga überträgt, trotz der schwerwiegenden Bedeutung einer solchen Entscheidung, wenn sie selbst gerade nicht verfügbar ist, die Verantwortung für die Genehmigung des Einsatzes von Spähsoftware gegen Bürger dem Staatssekretär des Justizministeriums, dessen Amt derzeit Robert Repassy ausübt[132]. Dies wurde von Repassy selbst in seiner Antwort auf eine schriftliche Anfrage zu diesem Thema bestätigt[133]. Es wird allgemein berichtet, dass Varga die Verantwortung regelmäßig an Repassys Vorgänger Pál Völner abgab, der aufgrund eines großen Korruptionsskandals im Dezember 2021 gezwungen war, vom Amt zurückzutreten[134]. Es wurde allgemein berichtet, dass er Bestechungsgelder in Höhe Millionen ungarischer Forint von einer Reihe wichtiger Interessenträger als Gegenleistung für günstige Entscheidungen und Verleihung wichtiger Ämter durch seine Befugnisse als Staatssekretär akzeptierte[135].

92. Zwar besteht Innenminister Sándor Pintér darauf, dass dieses Genehmigungsverfahren über den Minister oder die Gerichte immer ausnahmslos befolgt wird, doch ermöglichen[136]die schwachen gesetzlichen Bestimmungen des Gesetzes zur nationalen Sicherheit es den Generaldirektoren des SNSS auch, eine vorläufige Genehmigung für die Durchführung der Überwachung ohne Zustimmung zu erteilen, bis eine behördliche Genehmigung erteilt werden kann. Dies ermöglicht es dem SNSS, ohne ordnungsgemäße gerichtliche Genehmigung zu arbeiten, solange er geltend macht, dass die Verzögerung bei der Einholung der Genehmigung ihrem Betrieb schaden würde. In solchen Fällen kann die unbefugte Überwachung fortgesetzt werden[137].

93. Die gesetzlich vorgeschriebene Höchstdauer von 90 Tagen für die Überwachung nach Gesetz kann auf einen einfachen Antrag eines Generaldirektors an den bevollmächtigten

---

[128] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Sections 56-58.
[129] Europe's PegasusGate: Countering Spyware Abuse - EPRS Report, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, Juli 2022 S. 20.
[130] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Sections 57 and 58.
[131] European Commission Rule of Law Report 2022, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf, at pg. 26.
[132] https://telex.hu/belfold/2021/12/10/repassy-robert-igazsagugyi-allamtitkar-varga-judit-igazsagugyi-miniszterium; Europe's PegasusGate: Countering Spyware Abuse, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, July 2022, at p. 20.
[133] https://telex.hu/belfold/2022/01/27/varga-judithoz-kerulhetett-vissza-a-titkos-megfigyelesek-engedelyezese.
[134] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye; https://hungarytoday.hu/444-key-figure-in-volner-corruption-case-gyorgy-schadl-judge-fired-judiciary-obh/.
[135] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye
[136] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 November 2021.
[137] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, at Section 59.

Beamten um weitere 90 Tage verlängert werden[138], was nur dazu dient, um den Anschein eines rechtlichen Schutzmechanismus zu erwecken.

94. Darüber hinaus besteht die Aufgabe der NAIH darin, die gesamte Überwachung durch die Nachrichtendienste zu kontrollieren. Der Präsident der NAIH, Attila Péterfalvi, machte fortlaufend geltend, dass jegliche Einsätze von Pegasus zu Zwecken der nationalen Sicherheit erfolgten, die in die ausschließliche Zuständigkeit der nationalen Regierungen fallen[139]. Die NAIH überprüfte das Zulassungsverfahren jedoch nur in technischer Hinsicht, um festzustellen, ob die Verarbeitung der Daten rechtmäßig war, und untersuchte nicht den Inhalt des Einsatzes von Pegasus. Die NAIH sah nicht die Notwendigkeit, die Zielpersonen für Zeugenaussagen vorzuladen, da sie Zugang zu allen relevanten Dokumenten hatte. Nur die vom Justizminister genehmigten Fälle wurden untersucht, da die NAIH die von einem Richter erteilten Genehmigungen nicht untersuchen kann[140].Laut Péterfalvi habe die NAIH-Untersuchung weder illegale Aktivitäten noch Unvereinbarkeiten mit den Verkaufsbedingungen der NSO Group feststellen können[141].

95. Da der Leiter der NAIH vom Ministerpräsidenten ernannt wird, kann ihre Unabhängigkeit in Frage gestellt werden[142]. Der EGMR entschied in dieser Angelegenheit im September 2022 in dem Fall *Hüttl*/*Ungarn*, der vom Anwalt der Ungarischen Zivilrechtsunion (HCLU) Tivadar Hüttl[143] zur Sprache gebracht wurde, als der Nationale Sicherheitsausschuss nach seiner angeblichen Abhörung beschloss, keine weiteren Ermittlungen einzuleiten und keine weiteren Rechtsbehelfe zur Verfügung standen[144]. Der EGMR stellte in seinem Urteil fest, dass die NAIH, obwohl sie berechtigt ist, die Handlungen der Geheimdienste zu untersuchen, nicht in der Lage gewesen sei, eine unabhängige Kontrolle des Einsatzes der Überwachung durchzuführen. Das Gericht stellte fest, dass der NAIH die hierfür erforderliche Zuständigkeit fehlte, da die Nachrichtendienste das Recht hätten, den Zugang zu bestimmten Dokumenten auf der Grundlage der Geheimhaltung zu verweigern[145]. In einem solchen Fall wäre es Sache des für die Geheimdienste zuständigen Ministers, ein Audit durchzuführen, was in keiner Weise als unabhängige Kontrolle angesehen werden könnte[146].

EX-POST-KONTROLLE

96. Im November 2021 führten der Ausschuss für die nationale Sicherheit und der

---

[138] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, at Section 58.
[139] HVG, https://hvg.hu/itthon/20111117_Peterfalvi_palyaja_adatvedelem, 21. November 2011.
[140] Informationsreise des PEGA-Ausschusses nach Ungarn, 20. Februar 2023.
[141] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 February 2022.
[142] https://hclu.hu/en/pegasus-whats-new.
[143] https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-219501%22]}.
[144] https://tasz.hu/cikkek/valoszinusithetoen-lehallgattak-pert-nyert-strasbourgban-a-tasz-ugyvedje; https://hudoc.echr.coe.int/fre?i=001-219501.
[145] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere.
[146] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere.

Ausschuss für Verteidigung und Sicherheit in der Nationalversammlung auf Drängen der Opposition Anhörungen über den Einsatz von Spähsoftware in Ungarn und die angeblich politisch motivierte gezielte Überwachung von Bürgern durch die Regierung im Besonderen durch. Die Regierungspartei hatte 4 von 6 Sitzen im Ausschuss für die nationale Sicherheit und verhinderte jede sinnvolle und demokratische Kontrolle des Einsatzes von Pegasus**.** Die Regierungsvertreter bestanden darauf, dass alle Überwachungen über die entsprechenden Kanäle genehmigt wurden, weigerten sich jedoch, sich dazu zu äußern, ob Journalisten oder Politiker zur Zielscheibe geworden waren. Sie weigerten sich ebenfalls, zu der Tatsache Stellung zu nehmen, dass die Genehmigungen vom Justizminister an den Staatssekretär Pál Völner übertragen worden seien, gegen den wegen Korruption und Machtmissbrauch ermittelt wird. Sie lehnten auch Anträge der Oppositionsmitglieder ab, eine eingehende Untersuchung durchzuführen und einzelne Agenten der Sicherheitsdienste zu befragen. Wichtige Zielpersonen wie Zoltán Varga und Szabolcs Panyi wurden vom Ausschuss nicht angehört. Im August 2021 wurde nur eine Proforma-Ermittlung durchgeführt, da dies die einzige Maßnahme war, die von der Mehrheit unterstützt wurde[147]. Es ist jedoch nicht möglich, genau zu wissen, was gesagt wurde, da die Regierungspartei das Protokoll der Sitzung bis 2050 unter Verschluss hält[148].

97. Nach Anschuldigungen von mindestens zehn Anwälten, dem Präsidenten der ungarischen Anwaltskammer und mindestens fünf Journalisten, die zur Zielscheibe geworden waren, wurde eine Untersuchung der NAIH eingeleitet[149]. In dem daraus resultierenden Bericht, der am 31. Januar 2022 veröffentlicht wurde, wurde der Schluss gezogen, dass der Einsatz von Pegasus ausschließlich aus Gründen der nationalen Sicherheit erfolgt war.

98. In ähnlicher Weise schloss die ungarische Staatsanwaltschaft ihre Ermittlungen zu den Zielen am 15. Juni 2022 ab und kam zu dem Schluss, dass keine unbefugte Überwachung stattgefunden habe.

99. Da das Justizministerium die Genehmigungsbefugnis besitzt und der von der Fidesz unterstützte Generalstaatsanwalt Péter Polt 2019 für weitere neun Jahre wiedergewählt wurde, nachdem er bereits für zwei Amtszeiten über insgesamt 15 Jahre das Amt innehatte, kann eine echte Kontrolle der Regierung in Frage gestellt werden.

100. Es gibt diesbezüglich keine Unterstützung innerhalb des ungarischen Antikorruptionsrahmens, da das Innenministerium, das ursprünglich Pegasus von der NSO Group erworben hat, für die Koordinierung der gesamten Antikorruptionspolitik und -kontrolle zuständig ist[150].

RECHTSBEHELF

---

[147] Informationsreise von PEGA nach Ungarn, Treffen mit Mitgliedern des Nationalen Sicherheitsausschusses des ungarischen Parlaments, 20. Februar 2023.
[148] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4. November 2021.
[149] Commission 2022 Rule of Law Report, https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, at p. 26.
[150] Commission 2022 Rule of Law Report, https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, at p. 10.

101. Als der Pegasus-Skandal in Ungarn ausbrach, gehörten Journalisten zu den Gruppen, die von der Regierung vorrangig ins Visier genommen wurden. Infolgedessen leitete Anfang 2022 eine Gruppe von sechs Journalisten und Aktivisten rechtliche Schritte vor den ungarischen Behörden, der Kommission und der EGMR ein. Die Hungarian Civil Liberties Union (HCLU) vertritt die Journalisten Brigitta Csikász, Dávid Dercsényi, Dániel Németh und Szabolcs Panyi sowie Adrien Beauduin, einen belgisch-kanadischen Doktoranden und Aktivisten. Der sechste Kläger möchte anonym bleiben. Die HCLU arbeitet auch mit Eitay Mack in Israel zusammen, um eine Klage beim Generalstaatsanwalt einzureichen, damit eine Untersuchung gegen die NSO Group eingeleitet wird[151].

102. Das Verfahren für diesen Fall wird bei den ungarischen Gerichten durch viele technische Aspekte blockiert. Da es in diesem Bereich keine umfassende Rechtsprechung gibt, sind die Verfahren unklar. Beispielsweise sind Fragen im Zusammenhang mit der Gerichtsbarkeit aufgetreten. Solche Handlungen und ständige Verzögerungen werden in erster Linie als Versuche angesehen, den Fall in einer technischen oder verfahrenstechnischen Frage abzuweisen.

103. Es gibt auch ein ernstes Problem in Bezug auf den Zugang zu Informationen. Um Zugang zu den Dateien zu beantragen, die alle von einem einzelnen Bürger gesammelten Daten enthalten, ist es erforderlich, den genauen Namen der Akte anzugeben, auf die sich der Antrag bezieht. Diese Information zu erhalten, ist beinahe unmöglich. Da die Anträge der sechs von der HCLU vertretenen Parteien unweigerlich vom Obersten Gerichtshof zurückgewiesen wurden, ersuchte die HCLU um ein Urteil des Verfassungsgerichts, in dem diese Praxis erklärt wurde, und das Urteil des Obersten Gerichtshofs Ungarns, das für verfassungswidrig erklärt wurde. Im Jahr 2021 lehnte das Verfassungsgericht den Antrag der HCLU jedoch ab.

104. Neben ihren Klagen vor Gericht hat die HCLU auch andere Wege verfolgt, um auf die Daten ihrer sechs Mandanten zuzugreifen. Ein Verwaltungsverfahren wurde eingeleitet und gemäß dem Gesetz über Verschlusssachen und dem Datenschutzgesetz angenommen. Bevor Ergebnisse zustandekommen können, wird das Verfassungsschutzamt jedoch in jedem Einzelfall eine einjährige Überprüfung durchführen[152]. Darüber hinaus wurden die Spähsoftware-Angriffe dem Kommissar für Grundrechte (Ombudsman) gemeldet. Das Verfassungsgericht legte fest, dass der Ombudsmann dafür zuständig ist, Missbrauch durch die Geheimdienste zu untersuchen[153].

105. In einem weiteren Versuch, eine gewisse Transparenz zu erreichen, hat die HCLU den Zugang zu den Daten beantragt, die durch Hackerangriffe auf die sechs Zielpersonen gewonnen wurden und in einem Prozess, der außerhalb des Gerichtssystems durchgeführt wird, erhoben und verarbeitet werden. Der Anspruch auf diese Informationen besteht jedoch nur, solange die Übermittlung der Daten an die Betroffenen nicht die nationale Sicherheit beeinträchtigt[154]. Dies schafft einen weiteren

[151] The Guardian, https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state, *28 Januar 2022*.
[152] https://hclu.hu/en/pegasus-case-hungarian-procedures.
[153] https://hclu.hu/en/pegasus-whats-new.
[154] https://hclu.hu/en/pegasus-case-hungarian-procedures.

Vorwand für die ungarischen Behörden, wieder auf Gründe der nationalen Sicherheit zu verweisen[155]. Bisher hat das Verfassungsschutzamt 270 Auskunftsanfragen der HCLU zwischen 2018 und Mai 2022 abgelehnt[156].

POLITISCHE KONTROLLE

106. Die politische Kontrolle über den Einsatz der Überwachung in Ungarn ist allumfassend und total. Das von Orbán geführte Fidesz-Regime hat ein Kontrollsystem eingerichtet, mit dem es Anwälte, Journalisten, politische Gegner und Organisationen der Zivilgesellschaft mit Leichtigkeit und ohne Angst vor Regressansprüchen ins Visier nehmen kann.

107. Der Innenminister war ursprünglich für den Erwerb der Spähsoftware Pegasus verantwortlich und der Justizminister ist weiterhin dafür zuständig, deren Einsatz zu genehmigen. Ungarns Rechtsrahmen für die Überwachung seiner Bürger wurde wiederholt als mangelhaft befunden. Die regierende Partei wird jedoch keine Schritte unternehmen, um ihn zu ändern, da er ihrer eigenen Agenda zuträglich ist.

108. Der Ministerpräsident benennt den Leiter der NAIH, die Behörde, für die unabhängige Überwachung der Nutzung von Pegasus durch die Nachrichtendienste verantwortlich ist. Da es sich dabei um einen politischen Benannten handelt, ist eine unabhängige Kontrolle nicht vorhanden. Derartige politische Benennungen sind für Ungarn und die Fidesz-Partei nicht unüblich. Die Regierung hat Loyalisten systematisch in Führungspositionen in Gremien wie dem Verfassungsgericht, dem Obersten Gerichtshof, dem Rechnungshof, der Staatsanwaltschaft, der ungarischen Nationalbank und dem Nationalen Wahlausschuss eingesetzt[157]. Dadurch wird sichergestellt, dass jede Institution, die mit der Absicht gegründet wurde, die Exekutive zu kontrollieren, ihre Rolle nicht unabhängig wahrnehmen kann[158].

109. Telekommunikationsunternehmen spielen eine wichtige Rolle bei der praktischen Durchführung der Überwachung durch Spähsoftware. Es gibt mehrere Fälle, in denen Zielgeräte über per SMS gesendete Links infiziert wurden, und die Fülle an Daten, auf die Telekommunikationsunternehmen Zugriff haben, ist für diejenigen, die eine Überwachung durchführen möchten, sehr attraktiv. Im Falle Ungarns ist die Situation gefährlicher geworden, da die ungarische Regierung kürzlich den Telekommunikationsanbieter Vodafone Ungarn gekauft hat[159]. Mit Unterstützung der ungarischen Regierung kaufte das Unternehmen 4iG 51 % von Vodafone über eine Tochtergesellschaft. Darüber hinaus kaufte die ungarische Regierung 49 % der Anteile von Vodafone über ein anderes Unternehmen. Die Verbindungen zwischen 4iG und der Regierung sind offensichtlich. Der derzeitige Vorsitzende des Unternehmens war ein

[155] https://hclu.hu/en/pegasus-whats-new.
[156] https://hclu.hu/en/pegasus-whats-new.
[157] Martin, J and Ligeti, M., 'Hungary. Lobbying, State Capture and Crony Capitalism', Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. and Harris, P. (eds.), Springer, 2017, pp. 177-193, at p. 178.
[158] Martin, J. and Ligeti, M., 'Hungary. Lobbying, State Capture and Crony Capitalism', Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. and Harris, P. (eds.), Springer 2017, pp. 177-193 at p. 178.
[159] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22 August 2022.

enger Vertrauter des ungarischen Oligarchen Lőrinc Mészáros, eines Jugendfreunds von Viktor Orbán. Dieser Kauf, dessen gesamte Anschaffungskosten sich auf 1,7 Milliarden Euro beliefen, wird der Regierung einen einfachen und direkten Zugriff auf die Daten von mehr als 3 Millionen Kunden gewähren[160]. Darüber hinaus wird der Staat aufgrund dieses Kaufs einen Zugangspunkt zum Jahrzehnte alten globalen Nachrichtensystem SS7 haben[161]. Dieses System ermöglicht es Mobilfunkbetreibern, Nutzer weltweit miteinander zu vernetzen. Der ungarische Staat wird auch in der Lage sein, einen solchen Zugangspunkt weiter zu verpachten, wie es bei Rayzone der Fall war[162].

DIE ZIELE

110. Berichten zufolge enthielten die Ergebnisse des Pegasus-Projekts die Telefonnummern von über 300 Personen[163]. Darunter befanden sich mindestens fünf Journalisten, zehn Anwälte, der Bürgermeister von Gödöllő, der Mitglied einer Oppositionspartei ist, ein Mitarbeiter der Oppositionspartei, sowie Aktivisten und Inhaber einflussreicher Unternehmen[164]. Jedoch war keiner von ihnen in strafrechtlichen Ermittlungen involviert oder irgendwelcher Verbrechen beschuldigt. Auch wenn nicht alle zu den auf der Liste aufgeführten Telefonnummern zugehörigen Telefone mit an Sicherheit grenzender Wahrscheinlichkeit gehackt wurde, ist es doch ein aufschlussreicher Einblick in das methodische und systematische Vorgehen und die Haltung der Regierung Orbán gegenüber den Grundrechten und der Medienfreiheit. Seit diesem Zeitpunkt im Jahr 2021 wurde mittlerweile bestätigt, dass eine Reihe von Zielpersonen tatsächlich mit Spähsoftware überwacht wurde. Es war von dem Moment an, als der Abhörskandal in Ungarn ans Licht kam, klar, dass das Vorgehen der Regierung politisch motiviert war.

SZABOLCS PANYI

111. Das Telefon des Journalisten und Redakteurs Szabolcs Panyi wurde im Rahmen seiner Tätigkeit bei Direkt36 gehackt. Als eine der wenigen verbliebenen unabhängigen Nachrichtenquellen in Ungarn stellt sie in den Augen der Regierungspartei ein Hauptziel für solche Angriffe dar. Panyi ist ein bekannter und geschätzter Journalist. Daraus folgt, dass nicht nur wichtige Informationen direkt über Panyi abgefangen werden können, sondern auch viele der Kontakte und Quellen auf seinem Telefon einen wertvollen Beifang für die Regierung darstellen könnten.

112. Amnesty International bestätigte, dass das Telefon von Panyi 2019 über einen Zeitraum von sieben Monaten hinweg konsequent gehackt wurde[165]. Diese Angriffe traten gezielt

[160] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22 August 2022; Volkskrant, Orbán verstevigt traf den Namen Vodafone Hongarije grip op Telecommunicatie, critici uiten zorgen.
[161] The Guardian, https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands, 16 December 2020.
[162] https://www.haaretz.com/israel-news/tech-news/2020-12-17/ty-article/israeli-spy-tech-firm-tracked-mobile-users-around-the-world-investigation-suggests/0000017f-e76b-da9b-a1ff-ef6f847c0000.
[163]Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[164] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. Juli 2021 und Washington Post,https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[165] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.

und oft in Momenten auf, in denen Panyi die Regierung aufgefordert hatte, zu Fragen Stellung zu nehmen. Ein konkretes und beunruhigendes Beispiel hierfür ereignete sich am 3. April 2019. Panyi kontaktierte die Regierung und bat um einen Kommentar zu dem Artikel, den er über den Umzug einer russischen Bank in die ungarische Hauptstadt geschrieben hatte. Dabei handelte es sich um ein brisantes Thema, da Unsicherheit darüber bestand, ob die Bank tatsächlich eine Front für die russischen Geheimdienste war oder nicht[166]. Amnesty International bestätigte, dass das Telefon von Panyi am folgenden Tag gehackt wurde, und bestätigte zusätzlich, dass unmittelbar infolge einer Bitte um Stellungnahme an Orbáns Regierung 11 andere solcher Fälle von Hacking auftraten[167]. Dies bedeutet, dass auf über die Hälfte der Anfragen von Panyi innerhalb dieses Zeitraums von sieben Monaten Hackerangriffe folgten[168].

113. Die Behörden haben Unwissenheit über den Angriff gegen Panyi vorgetäuscht und werden ihre Verantwortlichkeit weder bestätigen noch leugnen. Allerdings hat die Regierung Panyi zuvor öffentlich angegriffen, indem Orbáns Sprecher behauptete, er sei ein fanatischer politischer Aktivist, und ihn der Orbánophobie und Hungarophobie beschuldigte[169]. Dies ist ein offenkundiger Versuch, Panyi zu diskreditieren und sowohl seine Quellen als auch ihn selbst durch die eigenen staatlich kontrollierten Medien als „Feind“ der Regierung darzustellen.

114. Nach einer Untersuchung Panyis gegen das ungarische Brokerunternehmen Communication Technologies Ltd, über das Pegasus erworben wurde, verklagte ihn das Unternehmen[170].

ZOLTÁN VARGA

115. Als Geschäftsführer und Vorsitzender der Central Media Group ist Zoltán Varga Eigentümer von Ungarns größter verbleibender unabhängiger Nachrichtenseite 24.hu. Nachdem die Orbán-Regierung im Jahr 2020 die Übernahme des Hauptkonkurrenten Index.hu eingeleitet hatte, blieb Varga als „letzter Mann“ übrig und bot der Regierungspartei weiterhin die Stirn[171].

116. Fidesz führt seit einiger Zeit eine Verleumdungskampagne gegen Varga über die von der Regierung kontrollierten Medien durch, um sowohl seine Person als auch seine mit über 7.5 Millionen Lesern pro Monat sehr beliebte Nachrichtenseite zu diskreditieren[172]. Varga macht geltend, er sei bei verschiedenen Gelegenheiten sowohl dazu verleitet worden, als auch unter Drohung dazu gedrängt worden, zu verkaufen, und erhielt unter anderem Angebote für großzügige staatliche Werbesubventionen. Im Gegenzug dazu

[166] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[167] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[168] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[169] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[170] Informationsreise des PEGA-Ausschusses nach Budapest vom 20. bis 21. Februar 2023.
[171] https://www.mapmf.org/alert/25319.
[172] Politico, https://www.politico.eu/article/viktor-orban-bent-on-muzzling-independent-press-hungarian-media-mogul-warns-index-24-hu-news-sites/, 25 July 2020.

sollte er der Regierung erlauben, sein Redaktionspersonal auszuwählen[173]. Varga hegte erste Vermutungen, dass sein Telefon mit Pegasus infiziert war, als er während eines Anrufs eine Wiedergabe des Gesprächs hörte. Später im Jahr 2021 wurde von Amnesty International aufgedeckt, dass Varga höchstwahrscheinlich von Pegasus gehackt wurde, was aber nicht bestätigt werden konnte, weil das Telefon seitdem ersetzt worden war[174].

117. Darüber hinaus versuchte der wiedergewählte Orbán kurz nach den Wahlen 2018 indirekt zu Varga zu gelangen. Nach einem Abendessen anlässlich eines Gespräch über die Medienübernahme der Regierung, das im Frühjahr 2018 von Varga veranstaltet wurde und an dem auch Attila Chikán, ein zum Orbán-Kritiker gewordener ehemaliger Fidesz-Minister, teilnahm, wurde bestätigt, dass alle Anwesenden als potentielle Überwachungsziele registriert wurden[175]. Es wurde später bestätigt, dass ein Gast zum Zeitpunkt der Veranstaltung gehackt wurde, während andere Telefone Spuren von potenziellen Pegasus-Hacks zeigten, aber keinen Hinweis auf eine erfolgreiche Infektion[176]. Der Hackingangriff wurde von einer an der Regierung angeschlossenen Bekannten von Varga nahezu bestätigt, die im Gespräch direkt auf das Abendessen Bezug nahm und davor warnte, sich mit Menschen zu umgeben, die „gefährlich“ sein könnten[177].

118. Varga wurde auch auf herkömmliche Weise überwacht. Aufgrund von Abhörungen am Arbeitsplatz, Autos, die vor seinem Haus verweilten, Hubschrauber, die über seinem Haus schwebten, und mehrere Einfälle in seinen Garten, stellte er vollzeitbeschäftigtes Sicherheitspersonal ein.

119. Im Oktober 2022 wurden Strafanzeigen gegen Varga erstattet. Nur wenige Minuten, nachdem er von der Polizei zur Befragung vorgeladen wurde, berichteten die regierungsfreundlichen Medien darüber[178].

ADRIEN BEAUDUIN

120. Adrien Beauduin tauchte 2018 auf dem Radar des Orbán-Regimes auf, als er an der Central European University (CEU) in Gender Studies promovierte. Die Institution wurde von George Soros gegründet und die Regierung versuchte damals, sie aus Ungarn zu verbannen, ebenso wie das Fachgebiet der Gender Studies im Allgemeinen[179]. Nach seiner Teilnahme an einer Demonstration in Budapest wurde Beauduin in einer als politisch motiviert angesehenen Aktion verhaftet und wegen

[173] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[174] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[175] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[176] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[177] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[178] Informationsreise des PEGA-Ausschusses nach Budapest vom 20. bis 21. Februar 2023.
[179] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.

Angriffs auf einen Polizeibeamten angeklagt. Er bestreitet den Sachverhalt vehement[180]. Berichten zufolge lagen im Wesentlichen keine Beweise gegen Beauduin vor. Die vorgelegten Beweise sollen wortwörtlich von der Aussage eines Polizeibeamten in einem anderen Fall kopiert worden sein[181]. Im Jahr 2020 wurde das Strafverfahren gegen Adrien Beauduin, der in dem Fall durch die HCLU vertreten wurde, eingestellt.

121. Regierungsvertreter verurteilten öffentlich das so genannte pro-Einwanderungs-Netzwerk Soros‘ für die Orchestrierung „gewalttätiger Demonstrationen in Budapest“[182]. Anschließend wurden Spuren von Pegasus auf dem Telefon von Beauduin gefunden, es konnte jedoch nicht festgestellt werden, ob es erfolgreich infiziert worden war.

122. Da Beauduin belgischer Staatsbürger ist, der zum Zeitpunkt dieser Vorfälle in Ungarn lebte, kann die Bedeutung der grenzüberschreitenden Dimension dieses Falles nicht ausreichend betont werden. Sie ist entscheidend, da sie die souveränen Rechte der EU-Bürger, wie die Freizügigkeit und das Recht auf Arbeit, beeinträchtigt. Die Kommission verfügt über ein Beschwerdeverfahren, das jede Person in Anspruch nehmen kann, wenn ihre in der Charta verankerten Rechte verletzt wurden. Adrien Beauduin legte am 24. Januar 2022 eine solche Beschwerde ein. Sieben Monate später machte die Kommission jedoch in einem an seinen Anwalt gerichteten Antwortschreiben vom 17. August 2022 geltend, dass sie nicht befugt sei, zu intervenieren[183].

ILONA PATÓCS

123. Die Anwältin Ilona Patócs wurde im Sommer 2019 mutmaßlich mithilfe der Spätsoftware „Pegasus“ bespitzelt, als sie einen Mandanten in einem hochkarätigen, langwierigen Verfahren wegen Mordes vertrat[184]. Aufgrund der Art des von ihr verwendeten Mobilgeräts konnte jedoch nicht ermittelt werden, ob der Hacking-Angriff erfolgreich war bzw. wann genau dieser stattfand. Ihr Mandant, István Hatvani, hatte bereits sieben Jahre wegen Mordes verbüßt – die Verurteilung war laut Patócs „politisch motiviert“[185]. Obwohl eine andere Person nach dem Prozess den Mord gestand, schickte das ungarische Berufungsgericht Hatvani zurück ins Gefängnis, um seine ursprüngliche Strafe fertig abzusitzen. Die Liste der Telefonnummern, die potenziell mit der Spähsoftware „Pegasus“ abgehört wurden, umfasst auch die einer Reihe von Anwälten, darunter auch die des Präsidenten der ungarischen Anwaltskammer János Bánáti[186]. Dieses Vorgehen zeigt, dass die Regierung das Anwaltsgeheimnis zwischen Anwälten und ihren Mandanten eindeutig missachtet.

---

[180] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 Juli 2021.*
[181] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 Juli 2021.*
[182] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 Juli 2021.*
[183] https://tasz.hu/a/files/220816-Complaint-unlawful-surveillance.pdf.
[184] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 März 2022.
[185] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 März 2022.
[186] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 März 2022.

GYÖRGY GÉMESI

124. György Gémesi, der Bürgermeister von Gödöllő, wurde Ende 2018 ebenfalls von der Pegasus-Spähsoftware ins Visier genommen. Zu diesem Zeitpunkt stand er unter starkem Druck der Regierung und unbekannte Personen brachen in seine Wohnung sowie die Wohnungen seiner Kinder ein. Zur gleichen Zeit wie der Oppositionsbürgermeister wurde Ende 2018 auch eine in der Regierung tätige Bekanntschaft Gémesis Ziel der Spähsoftware. Darüber hinaus standen zwei Telefonnummern seiner Parteikollegen und Gémesis ehemaliger stellvertretender Bürgermeister auf der Liste.

BRIGITTA CSIKÁSZ

125. Während ihrer Überwachung recherchierte Brigitta Csikász, eine der erfahrensten Kriminalreporterinnen in Ungarn, unter anderem den Missbrauch von EU-Geldern. Die Ermittlungen von Csikász ergaben, dass trotz der Warnungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) den ungarischen Behörden entweder der Wille oder die Möglichkeit fehlte, die verdächtigen Ausgaben von EU-Geldern zu verfolgen, was wiederum beweist, dass die Strafverfolgung zwar de jure unabhängig und stark hierarchisch aufgebaut ist, der oberste Staatsanwalt de facto jedoch eng mit der Regierungspartei und dem Ministerpräsidenten verbunden ist.

126. Der Präsident der ungarischen Anwaltskammer, János Bánáti, Strafverteidiger und mehrere andere Anwälte wurden ebenfalls von Pegasus angegriffen.

WEITERE ZIELE

127. Auch Personen aus dem Umfeld der Regierungspartei wurden von Spähsoftware bespitzelt. Die unabhängige ungarische Zeitung Direkt36 berichtete im Dezember 2021, dass ein Leibwächter des Präsidenten und engen Verbündeten von Orbán, János Áder, Opfer eines Hackerangriffs mit der Spähsoftware „Pegasus“ geworden war. Der Direkt36-Journalist Szabolcs Panyi, der Opfer eines Angriffs mit Spähsoftware wurde, äußerte sich dahingehen, dass diese Art von Ausspähung vor allem auf die wachsende Paranoia des ungarischen Premierministers zurückzuführen sei. Cecília Szilas, die ehemalige Botschafterin Ungarns in China, wurde kurz vor ihrer Tätigkeit als Beraterin von Viktor Orbán von Pegasus angegriffen. Attila Aszódi, der Staatssekretär der Regierung von Orbán, der für den Errichtung und die Entwicklung des von Roszatom zu bauenden Kernkraftwerks Paks II verantwortlich ist, wurde ebenfalls von der Spähsoftware Pegasus angegriffen. Der Angriff erfolgte 2018, als er Teil der Regierung war, aber sich mit seinem Vorgesetzten, Minister János Süli, im Konflikt befand.

128. Darüber hinaus wurden sowohl der Sohn als auch der Anwalt eines der ältesten Freunde Orbáns, Lajos Simicska, von Pegasus gehackt[187]. Simicska wurde von einem engen Freund von Orbán zu seinem Gegner. Er war dabei, sein Medienkonsortium zu verkaufen, das nach Orbáns Wahlsieg 2018 einen Großteil der Fehde angeheizt hatte,

[187] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.

als dieser Angriff auf Personen in seinem engen Umfeld stattfand[188]. Simicska selbst wurde kein Opfer eines Hackingangriffs aus dem einfachen Grund, dass er kein Smartphone benutzt, was eine Infektion mit Spähsoftware wie Pegasus unmöglich macht[189]. Ajtony Csaba Nagy, Simicskas Anwalt, vermutete eine Infektion, als er während eines Telefonats eine Wiedergabe seines Gesprächs mit Simicska hörte. Später wurden diese Verdächtigungen scheinbar bestätigt, als Informationen, die nur in diesen Anrufen ausgetauscht worden waren, in den ungarischen Medien auftauchten[190]. Da sich die Mehrheit der Nachrichtenagenturen in Ungarn im Staatsbesitz befindet, ist es wahrscheinlich, dass die Regierung selbst die Informationen direkt den Medien zur Verfügung gestellt hat.

SPÄHSOFTWARE-FIRMEN

129. Die ungarische Regierung erwarb nicht nur die Spähsoftware „Pegasus“ und setzte diese gegen ihre Bürger ein. Ungarn diente auch als Brutstätte für andere Unternehmen der Geheimdienst-Branche wie Black Cube und Cytrox. Bei der Firma Black Cube handelt es sich um einen privaten israelischen Nachrichtendienst, für den ehemalige Mitarbeiter des Mossad, des israelischen Militärs und der israelischen Geheimdienste tätig sind[191]. Auf seiner eigenen Website bezeichnet sich das Unternehmen als „kreativer Nachrichtendienst“, der „maßgeschneiderte Lösungen für komplexe geschäftliche und rechtliche Herausforderungen“ findet[192]. Black Cube war in eine Reihe von öffentlichen Kontroversen um Hackerangriffe verwickelt, unter anderem in den USA und Rumänien[193]. Außerdem wurde aufgedeckt, dass das Unternehmen mit der NSO Group und Pegasus Spyware in Verbindung steht. Nach dem großen öffentlichen Druck in Bezug auf die Beauftragung von Black Cube durch NSO, um ihre Gegner ins Visier zu nehmen, räumte der ehemalige CEO von NSO Shalev Hulio ein, Black Cube in mindestens einem Fall in Zypern beauftragt zu haben.

130. Black Cube beteiligte sich an den Wahlen 2018 in Ungarn, indem sie verschiedene NGOs und Personen, die irgendeine Verbindung zu George Soros hatten, ausspionierten und Orbán davon berichteten, damit er ihre Aktivitäten für eine Verleumdungskampagne verwenden konnte[194]. Zu den Zielgruppen gehörten die Rechtsanwältin und Mitglied des ungarischen Komitees für Menschenrechte in Helsinki, Marta Pardavi[195]. Die aus der Überwachung gewonnenen Informationen dieser Personen und NGOs erschienen nicht nur in den ungarischen staatlich kontrollierten

[188] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[189] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[190] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[191] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7 Oktober 2019.
[192] https://www.blackcube.com/.
[193] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 April 2022.
[194] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 July 2018.
[195] *Reuters*, https://www.reuters.com/article/meta-facebook-cyber-idCNL1N2T12MC, 16 December 2021.

Medien, sondern auch in der Jerusalem Post[196].

131. Eine weitere Verbindung mit Ungarn ist die Cytrox Holdings Zrt., die mit eine Adresse in Budapest registriert ist. Cytrox, der Entwickler der Spähsoftware Predator, wurde ursprünglich in Nordmazedonien gegründet, bevor es von WiSpear gekauft wurde, das jetzt Teil der Intellexa Alliance von Tal Dilian ist.

ABSCHLIEßENDE BEMERKUNGEN

132. Der Einsatz von Pegasus in Ungarn scheint Teil einer kalkulierten und strategischen Kampagne zur Zerstörung der Medienfreiheit und Meinungsfreiheit durch die Regierung zu sein[197]. 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. Da die Regierung die Kontrolle über fast alle ungarischen Offline-Medien und ausgestrahlten Medien besitzt, ist es ihr möglich, ihre eigene Version der Wahrheit weiter voranzutreiben und zu verhindern, dass ein Großteil der durch die unabhängigen Medien ausgeführten öffentlichen Kontrolle die ungarischen Bürger erreicht.

133. 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[198][199]. 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,[200] obwohl die Regierung beharrlich darauf besteht, dass sie in allen Fällen rechtmäßig gehandelt hat und sich vollständig an das Gesetz hält[201][202]. Obwohl die Regierung immer wieder auf Gründe der „nationalen Sicherheit“ verweist[203], sind ihre Behauptungen, dass die Zielpersonen eine Bedrohung der nationalen Sicherheit darstellen, nicht glaubwürdig.

I. C. Griechenland

134. Der Ausschuss reiste im November 2022 im Rahmen einer gemeinsamen

---

[196] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 July 2018.
[197] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[198] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 July 2021.
[199] DW, ‘Pegasus scandal: In Hungary, journalists sue state over spyware’, 29 January 2022.
[200] Siehe u. a. Roman Zakharov v Russia [GC], no. 47143/06, ECHR 2015 39; Klass and others v. Germany, 6 September 1978, § 50, Series A no. 28. 40; Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003; Liberty and others v. United Kingdom, no. 58243/00, § 62, 1 July 2008.
[201] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 November 2021.
[202] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 Februar 2022.
[203] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 Februar 2022.

Informationsreise Griechenland-Zypern nach Griechenland. Die Mitglieder trafen sich mit Staatsminister Giorgos Gerapetritis und erörterten wichtige Überwachungsfälle sowie die Themen Medienpluralismus und Rechtsstaatlichkeit in Griechenland. Sie trafen sich auch mit Investigativjournalisten, Mitgliedern des griechischen Parlaments, dem Präsidenten der griechischen Datenschutzbehörde (HDPA), Vertretern der ADAE und NGOs sowie Menschenrechtsverteidigern.

135. Der Besuch verdeutlichte, dass mehr Anstrengungen zur Sicherstellung der Transparenz unternommen werden müssen. Die Vorwürfe des Missbrauchs der Überwachung und des Einsatzes von Spähsoftware müssen gegebenenfalls gründlich untersucht und sanktioniert werden. Alle erforderlichen Garantien sollten eingeführt werden, ebenso wie Reformen zur Verbesserung der Transparenz und zur Sicherstellung einer angemessenen gerichtlichen Aufsicht über den Einsatz der Überwachung gewährleisten. Der Besuch bestätigte ferner, dass klare Regeln erforderlich sind, um die Möglichkeit, die nationale Sicherheit als Grund für Überwachungstätigkeiten anzugeben, zu beschränken und eine ordnungsgemäße gerichtliche Kontrolle sowie ein gesundes, pluralistisches Medienumfeld sicherzustellen.

136. Im Jahr 2022 wurde Griechenland von einer Reihe von Berichten über den Einsatz von Spähsoftware erschüttert, der nach griechischem Recht illegal ist. Am 26. Juli 2022 reichte Nikos Androulakis, Mitglied des Europäischen Parlaments und Vorsitzender der griechischen Oppositionspartei PASOK, bei der Staatsanwaltschaft des Obersten Gerichtshofs eine Beschwerde über den Versuch ein, sein Mobiltelefon mit der Spähsoftware „Predator“ zu infizieren[204]. Der Versuch, sein Mobiltelefon mit einer Spähsoftware zu infizieren, wurde bei einer Überprüfung des Telefons von Herrn Androulakis durch den IT-Dienst des Europäischen Parlaments entdeckt[205]. Laut forensischer Analyse des IT-Dienstes fanden die versuchten Hacking-Angriffe in der Zeit statt, als Androulakis für den Vorsitz der Oppositionspartei kandidierte. Durch diese Enthüllung wurden die Beschwerden, die der Finanzjournalist Thanasis Koukakis im April und Mai 2022 eingereicht hatte, weil sein Telefon mit der Spähsoftware „Predator“ infiziert worden war, ins Rampenlicht gerückt. Die Infektion seines Telefons wurde von CitizenLab bestätigt. Im September machte der ehemalige Infrastrukturminister und Gesetzgeber der Syriza-Partei, Christos Spirtzis[206], geltend, ebenfalls von der Spähsoftware Predator angegriffen geworden zu sein. Obwohl sein Mobiltelefon nicht offiziell überprüft wurde, teilte Herr Spirtzis die Links, die er erhalten hatte, mit zwei Technikern, die ihm mündlich bestätigten, dass er angegriffen worden war[207]. Außerdem wurde später im selben Monat bekannt, dass der griechische Geheimdienst (EYP) angeblich zwei seiner eigenen Mitarbeiter mit Spähsoftware ausspioniert hatte[208]. Am 5. und 6. November enthüllten die griechischen Medien eine Liste von 33 Zielpersonen, bei denen es sich allesamt um hochrangige Persönlichkeiten handelte[209]. Die Liste – deren Verifizierung durch die Regierung und die Betroffenen noch aussteht – enthält Namen von Personen, die in der Politik, Wirtschaft und

[204] Euractiv, EU Commission alarmed by new spyware case against Greek socialist leader.
[205] Tagesspiegel, Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.
[206] *Reuters*, One more Greek lawmaker files complaint over attempted phone hacking.
[207] https://insidestory.gr/article/predator-perissoteroi-apo-20-oi-stohoi-toy-stin-ellada-symfona-me-tin-arhi-prostasias.
[208] Efsyn, Targeting the disliked.
[209] Documento, Apocalypse: They Watched – This Sunday in Document.

Medienlandschaft in Griechenland tätig sind. Die Auswirkungen dieses mutmaßlichen Einsatzes von Spähsoftware gehen weit über die Personen auf der Liste hinaus, da alle ihre jeweiligen Kontakte und Verbindungen indirekt ebenfalls von der Ausspähung betroffen sind, einschließlich ihrer Kontakte in EU-Gremien. Die weite Verbreitung von Spähsoftware wurde bereits im Meta-Bericht 2021 deutlich, in dessen Anhang 310 gefälschte Websites mit Links zur Spähsoftware „Cytrox“ aufführt wurden, von denen allein 42 eingerichtet wurden, um Zielpersonen in Griechenland in die Irre zu führen[210][211]. Ende November 2022 veröffentlichte die griechische Zeitung *Documento* eine Liste von 498 URLs, die für Überwachungstätigkeiten mit Predator verwendet wurden. Einige der URLs waren identisch mit denen, die im Meta-Bericht 2021 veröffentlicht wurden[212]. Am 28. Februar 2023 bestätigte der Präsident der HDPA, dass 300 Textnachrichten im Zusammenhang mit der Spähsoftware Predator an rund 100 Geräte gesendet wurden. Der Präsident der ADAE erklärte außerdem, dass die ADAE auf mehrere Beschwerden reagiert habe und zwei Fälle des Einsatzes von Predator und sowie eine Bankkontonummer einer Person, die mit den falschen Textnachrichten in Verbindung steht, identifiziert habe. Die Untersuchung der ADAE zu neuen Beschwerden ist im Gange[213].

137. Im August 2022 räumte die griechische Regierung ein, dass der EYP tatsächlich Herrn Androulakis und Herrn Koukakis überwacht habe, bestritt aber, dass sie jemals die Spähsoftware Predator eingesetzt oder erworben habe. Darüber hinaus wurden in diesem Zeitraum weitere Fälle von Überwachung durch den EYP bekannt, wie der des Journalisten Stavros Malichoudis[214]. Bis heute wurden keine offiziellen Gründe für die Überwachung bekannt gegeben.

138. Am 8. August 2022 veröffentlichte Ministerpräsident Mitsotakis eine Videobotschaft, in der er die uneindeutige Erklärung abgab, die Überwachung von Herrn Androulakis sei „rechtmäßig“, aber „politisch inakzeptabel“ gewesen. Er verwies weder auf die Überwachung von Herrn Koukakis noch auf die anderen mutmaßlichen Fälle. Er erklärte auch, dass er von der Überwachung nicht gewusst habe, sie aber nicht zugelassen hätte, hätte er davon gewusst[215]. Nach der offiziellen Erklärung des Regierungssprechers Yiannis Oikonomou versuchte Staatsminister Giorgos Gerapetritis, sobald der Ministerpräsident von Herrn Androulakis’ „rechtmäßiger Abhörung“ erfahren hatte, diesen vollständig über die Gründe seiner Überwachung zu informieren[216]. Herr Androulakis lehnte das Angebot ab, informiert zu werden, indem er erklärte, dass eine solche private Unterrichtung rechtswidrig sei und dass der einzige rechtmäßige Weg durch das griechische Parlament führte. Später erklärte Minister Gerapetritis in seiner Aussage vor dem Parlament, dass er nie von den Gründen gewusst habe, und bat darum, dass alle relevanten Informationen streng geheim gehalten

[210] Meta, Threat Report on the Surveillance-for-Hire Industry.
[211] Inside Story, Who was tracking the mobile phone of journalist Thanasis Koukakis?.
[212] Documento, 27. November 2022.
[213]Meinungsaustausch des PEGA-Ausschusses mit Konstantinos Menoudakos und Christos Rammos, 28. Februar 2023.
[214] Solomon, Solomon’s reporter Stavros Malichudis under surveillance for ‘national security reasons’; Ekathimerini, Wiretapping case: The phone data that triggered developments; EPRS. Greece’s Predatorsgate: The latest chapter in Europe’s spyware scandal?.
[215] *Reuters*, Greek PM says he was unaware of phone tapping of opposition party leader.
[216] 1b LIFO, Androulakis denied information in private upon his surveillance https://www.lifo.gr/now/politics/o-androylakis-arnithike-idiotiki-enimerosi-apo-ton-gerapetriti-kai-zita-na-toy.

werden. Der EYP steht nach einer Gesetzesänderung, die angenommen wurde, kurz nachdem seine Partei Néa Dimokratía im Jahr 2019 an die Macht kam, unmittelbar unter der Kontrolle von Premierminister Kyriakos Mitsotakis[217].

139. Nach den Enthüllungen traten sowohl Grigoris Dimitriadis, Generalsekretär der Regierung, der für die Zusammenarbeit zwischen der griechischen Regierung und dem EYP verantwortlich ist, als auch der EYP-Direktor Panagiotis Kontoleon zurück[218].

ERWERB

140. Ende 2019 stand Generalsekretär Dimitriadis in Kontakt mit der NSO Group, um die Spionagesoftware „Pegasus“ zu erwerben. Im Januar 2020 machte die NSO Group ein offizielles Angebot über eine Government-to-Government-Vereinbarung über 50 Mio. EUR. Nach der Unterzeichnung der Vereinbarung sollte die Einzelperson vom Vertrag zurücktreten und der EYP übernehmen. Der EYP würde bei der Installation des Systems mit dem Mossad zusammenarbeiten. Die Vereinbarung wurde schließlich abgebrochen[219].

141. Sowohl der EYP als auch die Regierung bestreiten kategorisch, dass Predator jemals von den griechischen Behörden erworben oder eingesetzt wurde[220]. Da es in den Fällen in Griechenland keine Beweise für die Identität des Käufers und Nutzers von Predator gibt, lässt sich nicht mit Sicherheit feststellen, ob oder wie die Regierung oder ein anderer Akteur Predator erworben hat. Wenn es jedoch nicht die griechische Regierung war, dann drängt sich der Schluss auf, dass ein nichtstaatlicher Akteur für die (versuchten) Hacking-Angriffe auf die Telefone von Koukakis und Androulakis verantwortlich gewesen sein muss. Dies würde nach griechischem Recht ein Verbrechen darstellen, das untersucht werden müsste. Die Hypothese, dass private Akteure hinter den Angriffen mit der Spähsoftware „Predator“ stecken, ist zudem höchst unplausibel, da sich dadurch die Auswahl der Zielpersonen nicht erklären ließe. Grundsätzlich ist es jedoch nicht unmöglich, Spähsoftware zu erwerben oder zu nutzen, ohne dass staatliche Stellen die Software direkt kaufen. Spähsoftware kann – wie bereits aus anderen Fällen bekannt – über Proxys, Maklerfirmen oder Mittelsmänner gekauft werden, oder es können Vereinbarungen mit Spähsoftware-Anbietern getroffen werden, damit diese bestimmte Dienstleistungen im Bereich Spähsoftware und Überwachung erbringen. Es besteht kein Zweifel daran, dass es enge Verbindungen und Abhängigkeiten zwischen bestimmten Personen und Ereignissen im Zusammenhang mit der Regierung, dem EYP und den Anbietern von Spähsoftware gab, insbesondere Krikel, einem bevorzugten Lieferanten für Kommunikations- und Überwachungsausrüstung unter anderem für die Polizei und den EYP. Krikel unterhält enge Verbindungen zu Personen aus dem Umfeld von Ministerpräsident Mitsotakis. Es gibt immer mehr Beweise für die vielschichtigen Beziehungen zwischen Intellexa, dem Unternehmen, das die Spähsoftware „Predator“ besitzt, und dem griechischen Staat. Am 16. Januar 2023 verhängte die griechische Datenschutzbehörde eine Geldstrafe von 50 000 EUR gegen Intellexa, weil das Unternehmen im Rahmen ihrer im Juli 2020 nach der Beschwerde von Herrn Androulakis eingeleiteten Untersuchung keine

[217] Euractiv, Another Greek opposition lawmaker victim of Predator.
[218] POLITICO, PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal.
[219] https://insidestory.gr/article/greek-state-and-spyware-vendor-intellexa-they-are-acquainted-after-all.
[220] EPRS. Greece’s Predatorsgate: The latest chapter in Europe’s spyware scandal?.

Informationen über ihre Klientel übermittelt hatte. Die entsprechenden Ermittlungen sind noch nicht abgeschlossen[221].

143. Eine Möglichkeit ist, dass Predator über Ketyak erworben wurde, einem Zentrum für technologische Unterstützung, Entwicklung und Innovation, das vom ehemaligen EYP-Chef Kontoleon gegründet wurde. Es ist unabhängig vom EYP tätig[222] und beteiligt sich an Projekten rund um Forschung, Innovation und Technologieentwicklung[223].

DIE ZIELE

GRIGORIS DIMITRIADIS

144. Dimitriadis ist der Neffe von Ministerpräsident Mitsotakis und war bis August 2022 war er Generalsekretär in dessen Büro. In dieser Funktion war er für die Kontakte der Regierung mit dem EYP verantwortlich. Er musste am 5. August 2022 zurücktreten, nachdem bekannt wurde, dass der EYP das Telefon von Herrn Androulakis abgehört hatte. Zunächst wurde sein Rücktritt auf das toxische politische Umfeld zurückgeführt, später aber wurde ihm die politische Verantwortung für das Abhören von Herrn Androulakis und anderen Politikern zugeschrieben[224].

145. Der ehemalige Leiter des EYP, Panagiotis Kontoleon, gab vor dem griechischen Parlamentarischen Untersuchungsausschuss seine „soziale Beziehung“ mit Herrn Dimitriadis zu. Herr Kontoleon wurde von der Mitsotakis-Regierung ernannt, doch um seine Ernennung zu ermöglichen, mussten einige Bestimmungen des Gesetzes angepasst werden[225].

146. Herr Dimitriadis ist auch in mehrfacher Hinsicht eng mit Felix Bitzios und Giannis Lavranos verbunden. Die drei Männer sind persönlich miteinander bekannt. Herr Dimitriadis und Herr Lavranos waren Trauzeuge des jeweils anderen („Koumbaroi“)[226] und Herr Dimitriadis ist der Pate des zweiten Kindes von Herrn Lavranos[227]. Herr Dimitriadis war auch durch Geschäftstransaktionen mit Herrn Bitzios’ Bruder indirekt mit Herrn Bitzios verbunden[228].

147. Damit steht er im Zentrum eines Geflechts beruflicher und persönlicher Verbindungen zu den Schlüsselfiguren bei Intellexa und Krikel sowie dem EYP.

148. Herr Dimitriadis ist Berichten zufolge auch mit Andreas Loverdos vertraut, dem Kandidaten für den Vorsitz der PASOK-KINAL-Partei im Jahr 2021.

FELIX BITZIOS

---

[221] https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-stin-intellexa-ae-gia-mi-synergasia-me-tin-arhi.
[222] https://www.tovima.gr/print/politics/to-trigono-lfpou-egkatestise-lfto-predator-crstin-ypiresia-crpliroforion-crkai-i-lista-crton-xeiriston-tou/.
[223] https://www.nis.gr/en/ketyak.
[224] https://www.iefimerida.gr/politiki/paraitisi-dimitriadi-klima-toxikotitas-ohi-predator?amp, https://primeminister.gr/2022/08/08/29961.
[225] *Ieidiseis*, SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up.
[226] TVXS, Giannis Lavranos: The koumbarias with Tsouvala and Dimitriadis.
[227] Ieidiseis, SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up.
[228] Reporters United, The Great Nephew and Big Brother.

149. Der Geschäftsmann Felix Bitzios war in den großen Skandal um die Verletzung von Kapitalkontrollen durch die Bank of Piraeus verwickelt. Bis zum Abschluss der Ermittlungen wurde das Vermögen von Bitzios eingefroren[229]. Bitzios hatte von einer Gesetzesänderung profitiert, die Premierminister Mitsotakis kurz nach seinem Amtsantritt im Jahr 2019 eingeführt hatte. Die umstrittene Änderung legte eine zeitliche Begrenzung für das Einfrieren von Vermögenswerten fest und ermöglichte so die Freigabe eingefrorener Vermögenswerte nach maximal achtzehn Monaten[230]. Dank der Änderung der Regierung Mitsotakis konnte das Vermögen von Bitzios freigegeben werden.

150. Herr Bitzios ist mit Zypern über seine auf Zypern registrierte Firma Santinomo und seine Verbindung zu Tal Dilian verbunden. Es scheint, dass Herr Bitzios maßgeblich an der Übertragung von Intellexa nach Griechenland beteiligt war[231].

151. Herr Bitzios besaß über seine Firma Santinomo 35 % der Aktien von Intellexa. Am 4. August 2022 ließ er jedoch die Übertragung all seiner Aktien auf Thalestris, die Muttergesellschaft von Intellexa, eintragen[232]. Die Eintragung der Übertragung fand nur wenige Tage nach den Enthüllungen des Hacking-Angriffs auf das Mobiltelefon von Androulakis statt. Die Übertragung selbst erfolgte jedoch angeblich am 28. Dezember 2020, mehr als 19 Monate zuvor. Bitzios distanzierte sich damit rückwirkend von 1/3 der gesamten Intellexa-Anteile, die er bis dahin besaß. Nichtdestotrotz war Bitzios von März 2020 bis Juni 2021 als stellvertretender Geschäftsführer für Intellexa tätig[233].

GIANNIS LAVRANOS

152. Giannis Lavranos war wegen Steuerhinterziehung angeklagt worden und der Journalist Koukakis hatte über Lavranos' Fall berichtet.

INTELLEXA

153. Die Spähsoftware „Predator" wird über Intellexa vertrieben, ein Konsortium von Spähsoftware-Anbietern mit Niederlassungen unter anderem in Zypern, Griechenland, Irland und Frankreich. Tal Dilian, der im Laufe seiner früheren Karriere bei den israelischen Streitkräften tätig war, gründete das Konsortium in Zypern. Seine zweite Ex-Frau, die polnische Staatsbürgerin Sara Hamou, ist eine zentrale Figur in diesem verschlungenen Netzwerk von Unternehmen. Tal Dilian hat zusätzlich auch die maltesische Staatsbürgerschaft angenommen. Die griechische Regierung erklärte, dass Intellexa zwei Ausfuhrgenehmigungen erteilt worden seien, von denen eine die Ausfuhr nach Madagaskar genehmigt habe. Darüber hinaus erteilte die griechische Regierung eine Ausfuhrgenehmigung für Predator in den Sudan. Es wurde nicht bestätigt, ob die Genehmigung an Intellexa oder ein anderes Unternehmen erteilt wurde. Intellexa hat Berichten zufolge auch seine Produkte nach Bangladesch exportiert.

154. Am 30. November 2022 enthüllte ein Untersuchungsbericht von Lighthouse Reports in

[229] Lexocology, Cyprus court offers directions to bank on ambit of freezing injunction.
[230] Financial Times, Greek law change viewed as backtracking on money laundering.
[231] Inside Story, Predatorgate: The second shareholder of Intellexa SA.
[232] Inside Story, Predatorgate: The second shareholder of Intellexa SA.
[233] https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae.

Zusammenarbeit mit der israelischen Zeitung *Haaretz* und dem griechischen Medienoutlet Inside Story, dass Tal Dilians Predator-Operationen in Griechenland angeblich in Verbindung mit einem Cessna-Jet standen, der zwischen April und August 2022 von Griechenland und Zypern nach Sudan flog. Angeblich lieferte dieser Jet heimlich und illegal hochwertige Überwachungstechnologie an die Milizen der Rapid Support Forces (RSF)[234]. Flugaufzeichnungen verknüpften den Privatjet, der über Zypern ein- und ausflog, mit Tal Dilian, einem ehemaligen hochrangigen israelischen Verteidigungsagenten, der 2019 die Intellexa Alliance mit Stützpunkten in Zypern und Griechenland gründete. Am 18. Februar 2023 bestätigte die Kommission, dass sie die nationalen Behörden Griechenlands und Zyperns zur Klärung dieser Angelegenheit kontaktiert hatte. Die Kommission erhielt jedoch keine Antwort[235]. Am 19. April 2023 bestätigte der griechische stellvertretende Außenminister Miltiadis Varvitsiotis, dass die griechische Regierung die Lizenz für den Export der Spähsoftware „Predator“ in den Sudan genehmigt habe. Der Minister bestreitet jedoch, dass Predator bei den jüngsten Zusammenstößen zwischen den sudanesischen Streitkräften und den RSF-Milizen im Sudan irgendeine Rolle gespielt habe[236].

155. Im Dezember 2022 teilte die griechische Regierung mit, dass sie Intellexa am 15. November 2021 zwei Ausfuhrgenehmigungen erteilt hatte. Laut dem Sprecher des griechischen Außenministeriums Alexandros Papaioannou genehmigte eine davon den Verkauf von Predator nach Madagaskar[237]. Die Genehmigung wurde trotz der schlechten Menschenrechtsbilanz des Landes erteilt[238] und steht möglicherweise in Konflikt mit der EU-Verordnung über doppelte Verwendungszwecke[239]. Der Generalsekretär für internationale ökonomische Angelegenheiten, Ioannis Smyrlis, der den Verkauf von Predator an Madagaskar genehmigte, gab seinen Rücktritt bekannt, nachdem diese Enthüllungen ans Licht kamen, und übernahm dann das Amt des stellvertretenden Generaldirektors der regierenden Partei Néa Dimokratía[240], wodurch er für die bevorstehenden Wahlen verantwortlich ist.

156. Neben dem Export von Spähsoftware zeigt ein Fall Berichten zufolge, dass Griechenland Fortbildungsreisen für die Verwendung von Spähsoftware veranstaltete. Im Juni 2021 kaufte Bangladesch ein Überwachungsfahrzeug von der zyprischen Firma Passitora. Dokumenten des Innenministeriums Bangladeschs zufolge wurden die Mitarbeiter des Nationalen Telekommunikationsüberwachungszentrums (NTMS)

---

[234] https://www.lighthousereports.nl/investigation/flight-of-the-predator/; https://www.haaretz.com/israel-news/security-aviation/2022-11-30/ty-article-magazine/.premium/jet-linked-to-israeli-spyware-tycoon-brings-spy-tech-from-eu-to-notorious-sudanese-militia/00000184-a9f4-dd96-ad8c-ebfcd8330000; https://insidestory.gr/article/flight-predator

[235] https://www.europarl.europa.eu/doceo/document/E-9-2022-003990-ASW_EN.html; Sitzung des PEGA-Ausschusses, 28. März 2023.

[236] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/; https://www.aa.com.tr/en/africa/greek-government-admits-opposition-s-claim-of-spyware-export-to-sudan/2876824

[237] *The New York Times*, 8 December 2022, ‘How the Global Spyware Industry Spiraled Out of Control’, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[238] *The New York Times*, 8 December 2022, ‘How the Global Spyware Industry Spiraled Out of Control’, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[239] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (OJ L 206, 11.6.2021, p. 1).

[240] *The National Herald*, ‘Top Greek Official Who Authorized Predator Spyware Sale Resigns’.

zwischen 2021 und 2022 in Griechenland für die Nutzung des Überwachungsfahrzeugs geschult. Das Fahrzeug kam schließlich im Juni 2022 in Bangladesch an[241].

KRIKEL

157. Krikel ist ein bevorzugter Lieferant von Ausrüstung für die griechischen Strafverfolgungs- und Sicherheitsbehörden. Es ist auch der griechische Vertreter von RCS Lab, einem italienischen Unternehmen, das Überwachungssoftware verkauft. Außerdem soll Giannis Lavranos über ein anderes Unternehmen namens Mexal zu 50 % Eigentümer von Krikel sein[242]. Es lässt sich wohl jedoch – trotz der zahlreichen Verträge mit staatlichen Behörden – nicht mit Sicherheit feststellen, wer letztlich der wirtschaftliche Eigentümer von Krikel ist.

158. 2014 wurde Giannis Lavranos' Unternehmen Ioniki Technologiki an Tetra Communications in London verkauft. Ioniki Techniologiki gehört zu den drei Unternehmen, die im selben Jahr Tetra-Kommunikationssysteme an das griechische Ministerium für Bürgerschutz gespendet haben[243]. Enthüllungen von Wikileaks zufolge hatte die griechische Regierung im Jahr 2014 auch Interesse an der italienischen Spähsoftware-Marke RCS Galileo von der Firma Hacking Team gezeigt, aber diese Software wurde nie erworben[244]. Die Spende von Tetra-Kommunikationssystemen wurde von einem in Florida ansässigen Unternehmen vermittelt, sodass die üblichen Ausschreibungsverfahren umgangen werden konnten. Die Spende an die griechische Regierung wurde 2017 angenommen. 2018 unterzeichnete Krikel einen Vertrag über Wartungsarbeiten und technischen Support in Höhe von 10,8 Mio. EUR. Der Verwalter von Krikel, Stanislaw Pelczar, unterzeichnete den Vertrag im Namen von Krikel, aber es ist davon auszugehen, dass Lavranos die ganze Zeit über informell an den Verhandlungen beteiligt war[245]. Krikel wurde zu einem wichtigen Zulieferer des griechischen Ministeriums für Bürgerschutz. Seit 2018 hat das Unternehmen sieben Verträge mit der griechischen Regierung unterzeichnet, von denen sechs geheim sind[246].

159. Das Unternehmen Krikel wurde auch zum Vertreter des italienischen Unternehmens RCS Lab in Griechenland. Im Juni 2021 erwarb der griechische Nachrichtendienst (EYP) über Krikel[247] ein Abhörsystem von RCS Lab[248]. Zu dieser Zeit war Dimitriadis für die Kontakte zwischen der Regierung und dem EYP verantwortlich. In einigen

---

[241] *Haaretz*, 'Israeli Spy Tech Sold to Bangladesh, World's Third-largest Muslim Country, Despite Dismal Human Rights Record'.

[242] Hier gibt es mehrere interessante Verbindungen. Lavranos verkaufte sein Familienhaus in Athen im April 2021 zu einem Preis unter dem Marktwert an Albitrum Properties. Der Vertreter von Albitrum Properties während des Verkaufs war der Halbbruder von Felix Bitzios, Theodoros Zervos. Albitrum ist ein zyprisches Unternehmen und hat als Anteilseigner Mexal Services Ltd. Mexal Services besitzt 100 % der Eneross Holdings Ltd. Eneross Holdings ist zusätzlich Besitzer von Krikel. Der eingetragene Firmensitz von Giannis Lavranos befindet sich an derselben Adresse wie Eneross Holdings und Mexal Services in Zypern. Siehe: Inside Story, 'Predatorgate's invisible privates', and TVXS, 'G. Lavranos behind KRIKEL – How the deception of the Parliament was attempted [Revealing documents]'.

[243] Inside Story, 'Predatorgate's invisible privates'.

[244] Inside Story, 'The timeless interest of the Greek authorities in spyware'.

[245] Inside Story, 'Predatorgate's invisible privates'.

[246] Inside Story, 'Predatorgate's invisible privates'.

[247] TVXS, 'G. Lavranos behind KRIKEL – How the deception of Parliament was attempted [Revealing documents]'.

[248] *Hellas Posts English*, 'The EYP supplier contaminates smartphones in Greece as well'.

Quellen ist dokumentiert, dass während der Installation dieses neuen Systems Material mit Informationen über die Überwachung von Androulakis und Koukakis verloren gegangen ist – angeblich aufgrund eines technischen Problems[249]. Andere Quellen behaupteten jedoch, dass Kontoleon die Vernichtung von Akten am 29. Juli 2022 angeordnet habe[250].

160. Interessanterweise wurden Mitarbeiter von Krikel bei der Arbeit für Ketyak gesichtet, die sie angeblich unentgeltlich entrichteten. Ketyak hat offenbar im Rahmen eines vertraulichen Ausschreibungsverfahrens, das auf einer geheimen Entscheidung des Premierministers beruht, 40 Mio. EUR von der Aufbau- und Resilienzfazilität der EU (RRF) erhalten[251]. Die rechtswidrige Verwendung von EU-Mitteln zur Finanzierung illegaler Spähsoftware würde einen schwerwiegenden Verstoß gegen das Unionsrecht darstellen und in die Zuständigkeit zahlreicher Einrichtungen der EU, einschließlich der Europäischen Staatsanwaltschaft, fallen.

161. Berichten zufolge besuchten Krikel-Mitarbeiter im Dezember 2021 und Januar 2022 in ihrer Rolle als „Ausbilder“ auch EYP-Anlagen in Agia Paraskevi. Diese Einrichtungen werden von der griechischen Regierung kontrolliert und sind angeblich der Ort, an dem die Spähsoftware „Predator“ installiert wurde[252].

VERWICKLUNG VON BITZIOS UND LAVRANOS

162. Bitzios und Lavranos waren beide aktiv an der Gründung von Krikel im Jahr 2017 beteiligt. Gemeinsam leiteten sie die Ernennung des polnischen Anwalts Stanislaw Pelczar zum Verwalter von Krikel im Oktober 2017 in die Wege[253]. Bitzios Unternehmen Viniato Holdings Limited erhielt anschließend einen mit etwa 550 000 Euro Honorar dotierten Beratervertrag bei Krikel für den Zeitraum von Januar bis August 2018 (obwohl Krikel in diesem Jahr nur einen Umsatz von 840 000 Euro erzielte).[254]

163. Bitzios und Pelczar haben auch andere gemeinsame Geschäftsbeziehungen. Aus den Paradise Papers geht hervor, dass sie ein Unternehmen teilen, das in Malta unter dem Namen Baywest Business registriert ist[255]. Darüber hinaus besitzt Tal Dilian, der Gründer von Intellexa, einen maltesischen („goldenen“) Pass[256] sowie eine

[249] TVXS, ‘G. Lavranos behind KRIKEL – How the deception of Parliament was attempted [Revealing documents]’.
[250] Euractiv, ‘Greek MEP spyware scandal takes new turn’.
[251] https://www.flash.gr/politiki/1988373/predator-apokalypseis-gia-to-ketyak-tis-eyp-me-xrimatodotisi-kai-apo-to-tameio-anakampsis.
[252] Inside Story, ‘Greek State and spyware vendor Intellexa: they are acquainted after all’.
[253] TVXS, ‘G. Lavranos behind KRIKEL – How attempts were made to deceive the Parliament [Revealing documents]’.
[254] Inside Story, ‘From Koukakis to Androulakis: A new twist in the Predator spyware case’.
[255] International Consortium of Investigative Journalists, Offshore Leaks Database, Paradise Papers – Malta Corporate Registry.
[256] Government of Malta, Persons Naturalised Registered as Citizens of Malta, Gaz 21.12, https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf.

Briefkastenfirma in Malta, die MNT Investments LTD[257].

164. Bitzios und Lavranos sind zwei Schlüsselfiguren bei der Lieferung von Kommunikations- und Überwachungsmaterial an staatliche Stellen wie die Polizei und den EYP. Bitzios war eine Schlüsselfigur in dem Unternehmen, das Predator vertreibt. Beide standen Dimitriadis nahe und profitierten von lukrativen Regierungsverträgen. Ihnen spielte auch die Gesetzesänderung der neuen Regierung in die Karten, durch die ihre eingefrorenen Vermögenswerte freigegeben wurden. Sie hatten ein Motiv, Koykakis mithilfe von Spähsoftware zu bespitzeln. Diese Verflechtung von Geschäftsinteressen, persönlichen Beziehungen und politischen Verbindungen birgt ein sehr offensichtliches und hohes Risiko von Interessenkonflikten und Korruption. Diese beiden Männer wären des Weiteren in der Lage, entscheidende Informationen über den Erwerb und den Einsatz von Predator in Griechenland preiszugeben.

165. Trotz der offensichtlichen Relevanz möglicher Aussagen von Bitzios und Lavranos vor dem Untersuchungsausschuss des griechischen Parlaments lehnte die Néa Dimokratía-Mehrheit im Ausschuss die Anträge der Opposition ab, beide zu einer Anhörung vorzuladen.

EX-ANTE-KONTROLLE

166. In Griechenland stellt es gemäß mehrerer Artikel des griechischen Strafgesetzbuchs, darunter Artikel 292 über Straftaten gegen die Sicherheit des Telefonverkehrs, Artikel 292 B über die Beeinträchtigung des Betriebs von Informationssystemen sowie Artikel 370 über Verstöße gegen das Briefgeheimnis einen Straftatbestand dar, ein Gerät mit Spähsoftware zu infizieren. Darüber hinaus stellt die Herstellung, der Verkauf, die Lieferung, die Verwendung, die Einfuhr, der Besitz und die Verbreitung von Schadsoftware (einschließlich Spähsoftware) ebenfalls eine Straftat gemäß Artikel 292 C des griechischen Strafgesetzbuches dar[258]. Dieser Artikel wurde von der griechischen Regierung am 9. Dezember 2022 geändert.

167. Die Zahl der Genehmigungen für das Abhören von Telefongesprächen hat im Laufe der Jahre erheblich zugenommen, und zwar von 4 871 im Jahr 2015 auf 11 680 im Jahr 2019 und auf 15 475 im Jahr 2021.[259] Derzeit müssen rund 60 Anträge jeden Tag bearbeitet werden, bis vor kurzem von einem einzigen Staatsanwalt. Darüber hinaus werden in den Bestimmungen des EYP, nach denen aus Gründen der nationalen Sicherheit die Vertraulichkeit der Kommunikation von Bürgern aufgehoben werden kann, weder der Name der betroffenen Person noch der Grund für die Aufhebung der Vertraulichkeit genannt. Es werden nur die Telefonnummer und der Bezug auf die nationale Sicherheit erwähnt[260].

168. Die gerichtliche Befugnis zur Überwachung der privaten Kommunikation sowie die Verlängerung und Beendigung einer solchen Genehmigung müssen von der zuständigen

[257] https://mlt.databasesets.com/company-all/company/73006 https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/.
[258] International Comparative Legal Guide, *Cybersecurity Laws and Regulation Greece 2022*.
[259] Ekathimerini, 'Wiretapping and "national security"'.
[260] Reporters United, 'Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis'.

Staatsanwaltschaft genehmigt werden. Gemäß dem Gesetz 3649/2008 ist der für die Aufhebung der Geheimhaltung und Vertraulichkeit zuständige Staatsanwalt der interne Staatsanwalt des EYP. Eine Gesetzesänderung von 2018 unter der Regierung Tsipras II hatte die Zahl der Staatsanwälte, die für die Genehmigung eines Abhörvorgangs erforderlich sind, von zwei auf einen reduziert. Die für die vorliegenden Fälle zuständige Staatsanwältin ist Vasiliki Vlachou[261]. Vlachou traf sich nicht mit dem PEGA-Ausschuss in Griechenland.

GESETZGEBERISCHER AKT

169. Nach den Enthüllungen über die Überwachung hat Premierminister Mitsotakis Änderungen am Betriebsrahmen des EYP vorgeschlagen. Eine dieser Änderungen war die Einführung des Gesetzgeberischen Akts durch die Regierung am 9. August 2022. Artikel 9 Absatz 2 des Gesetzes Nr. 3649/2008 wurde dahingehend aktualisiert, dass nun eine Stellungnahme des Ständigen Ausschusses für Institutionen und Transparenz zur Ernennung des Gouverneurs des EYP erforderlich ist[262]. Da die Regierungspartei jedoch im Ständigen Sonderausschuss für Institutionen und Transparenz des Parlaments derzeit über eine absolute Mehrheit verfügt, hat sie für die Ernennung von Herrn Demiris zum neuen Gouverneur des EYP gestimmt, während alle ebenfalls dort vertretenen Oppositionsparteien dagegen gestimmt haben[263]. Zweiter stellvertretender Kommandant des EYP ist übrigens Dionysis Melitsiotis[264], ein ehemaliges Mitglied des Kabinetts des Premierministers, und Anastasios Mitsialis, ein ehemaliger Néa-Dimokratía-Funktionär, ist als weiterer stellvertretender Direktor tätig[265].

170. Darüber hinaus führte das Gesetz die Genehmigung von Überwachungsanträgen durch zwei Staatsanwälten wieder ein[266]. Artikel 5 des Gesetzes 3649/2008 über die Aufhebung der Vertraulichkeit von Mitteilungen durch den EYP wird durch eine Vorlage zur Genehmigung an die zuständige Staatsanwaltschaft der Berufungsinstanz ergänzt und danach vom Staatsanwalt des Berufungsgerichts genehmigt[267].

EX-POST-KONTROLLE

171. Seit 2019 unterstehen die Handlungen des EYP der direkten Kontrolle von Premierminister Kyriakos, nachdem das entsprechende Gesetz nach dem Sieg von Néa Dimokratía im Jahr 2019 geändert wurde[268].

172. Die parlamentarische Kontrolle wird vom Ständigen Ausschuss für Institutionen und Transparenz ausgeübt. Dieser Ausschuss überwacht die Handlungen des EYP und ist befugt, Dokumente zu sammeln, Personen zu befragen und den Generaldirektor zu einer

---

[261] Reporters United, ‘Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis’.
[262] EfSyn, ‘What (does not) change with the Act of Legislative Content for EYP?’.
[263] Ekathemirini, ‘Themistoklis Demiris: His appointment to the management of EYP was approved by a majority’.
[264] Ekathimerini, ‘National security takes center stage’.
[265] Greek City Times, ‘Greek PM appoints new security and intelligence chiefs’.
[266] At a Glance, ‘Greece’s Predatorgate: The latest chapter in Europe’s spyware scandal?’, European Parliament, Directorate-General for Parliamentary Research Services, 8 September 2022.
[267] EfSyn, ‘What (does not) change with the Act of Legislative Content for EYP?’.
[268] Euractiv, ‘Another Greek opposition lawmaker victim of Predator’.

Anhörung vorzuladen[269]. Die Regierungspartei hat in der derzeitigen Zusammensetzung des Ausschusses eine absolute Mehrheit.

173. Die griechische Behörde für Kommunikationssicherheit und Datenschutz (ADAE) stellt den Schutz des Briefgeheimnisses und allen anderen Arten von Kommunikation sicher[270]. Das Statut der ADAE gewährt ihr Verwaltungsautonomie[271]. Die ADAE kann Untersuchungen von Einrichtungen, Datenbanken und Archiven sowie der technischen Ausrüstung und Unterlagen des EYP durchführen[272].

174. Die im Gesetz Nr. 2225/1994 vorgesehenen Vorschriften zur Vertraulichkeit der Kommunikation besagen, dass eine Aufhebung dieser Vertraulichkeit nur in Fällen der nationalen Sicherheit und bei der Untersuchung schwerer Verbrechen möglich ist. Nach der Aufhebung der Vertraulichkeit sieht Artikel 5 dieses Gesetzes vor, dass die ADAE die Zielpersonen der Ermittlungen informieren kann, sofern der Zweck der Ermittlungen dadurch nicht beeinträchtigt wird[273]. Das Recht einer Person auf Zugang zu Informationen darüber, ob sie Gegenstand einer Überwachung war, ist im Gesetz Nr. 2472/1997 verankert[274]. Als jedoch im März 2021 die ADAE das EYP auf das Recht von Koukakis auf Information hinwies, legte die Regierung am 31. März 2021 sofort die Gesetzesänderung Nr. 826/145 vor, der die Möglichkeit der ADAE abschafft, Bürger über die Aufhebung der Vertraulichkeit der Kommunikation zu informieren[275]. Damit wird der Einzelne de facto seines Rechts auf Information beraubt. Die Änderung wurde auf höchst irreguläre Weise eingeführt. Sie wurde einem Gesetz hinzugefügt, das in keinem Zusammenhang mit dem Gesetz steht (einem Gesetzesentwurf zu Maßnahmen im Zusammenhang mit der COVID-19-Pandemie), und die von der Verfassung vorgeschriebenen Fristen wurden nicht eingehalten[276][277][278]. Es fand also kein ordnungsgemäßer Konsultationsprozess statt.

175. Mitsotakis zielte mit dem Gesetzgeberischen Akt darauf ab, Transparenz und Rechenschaftspflicht zu stärken. Mit dem Gesetz wird die Gesetzesänderung 826/145 jedoch nicht aufgehoben.

176. Am 9. Dezember 2022 verabschiedete die griechische Regierung das Gesetz 5002/2022, das einen aktualisierten, wirksamen Rechtsrahmen für den Schutz personenbezogener Daten, das Kommunikationsgeheimnis und die Stärkung der Cybersicherheit schaffen sollte. Mit dem Gesetz werden jedoch mehrere Bestimmungen eingeführt, die Garantien, Kontrollen und die Rechenschaftspflicht abschwächen.

---

[269] Centre for European Constitutional Law, *National intelligence authorities and surveillance in the EU:* Fundamental rights safeguards and remedies.
[270] ADAE, *Presentation*.
[271] ADAE*, Regulatory framework.*
[272] Centre for European Constitutional Law, *National intelligence authorities and surveillance in the EU:* Fundamental rights safeguards and remedies.
[273] Constitutionalism, 'Contradiction of Article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications'.
[274] Hellenic Data Protection Authority (DPA), Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data.
[275] https://www.reportersunited.gr/8646/eyp-koukakis/.
[276] Hellenic Parliament, Constitution.
[277] Hellenic Parliament, Rules of Procedure of the House.
[278] Govwatch, 'Violation of the legislative process for amendments in law 4790/2021'.

Gemäß Artikel 4 Absatz 7[279] werden alle Ersuchen von Einzelpersonen um Auskunft darüber, ob sie aus Gründen der nationalen Sicherheit überwacht wurden, von einem dreiköpfigen Ausschuss geprüft, der sich aus dem Direktor des EYP, der Staatsanwältin oder dem Staatsanwalt des EYP und dem Leiter der ADAE zusammensetzt. Dies bedeutet, dass die Entscheidungsmehrheit bei denen liegt, die die Überwachung überhaupt erst in Auftrag gegeben (der Direktor des EYP) und sie genehmigt haben (die Staatsanwältin/ der Staatsanwalt). Darüber hinaus ist es praktisch unmöglich, Personen, die aus Gründen der nationalen Sicherheit überwacht werden, nachträglich angemessen darüber zu informieren, da das Gesetz vorsieht, dass sie erst drei Jahre nach Beendigung ihrer Überwachung einen entsprechenden Antrag auf Ersuchen um Auskunft stellen dürfen. Dies ist mit der einschlägigen Rechtsprechung des Europäischen Gerichtshofs und der Europäischen Menschenrechtscharta[280] unvereinbar und sieht keine institutionellen Kontrollen vor, um das ordnungsgemäße Funktionieren der Staatsgewalt zu gewährleisten. Die ADAE hat zum Ausdruck gebracht, dass sie mit dem dreiköpfigen Gremium nicht einverstanden ist. Bisher gibt es keinen Handlungsrahmen für das dreiköpfige Gremium, was bedeutet, dass es de facto nicht funktioniert[281]. Darüber hinaus kriminalisiert das neue Gesetz die Verwendung von Spähsoftware durch den Einzelnen oder durch private Unternehmen und macht es zum ersten Mal für Behörden legal, Spähsoftware zu erwerben, was die Regierung ermächtigt, dies über ein Präsidialdekret anzuordnen. Es gibt keine Bestimmung für die gerichtliche Überwachung der Verwendung von Spähsoftware oder für die Vergabe von Abhöraufträgen an private Einrichtungen.

177. Die Lieferung von Spähsoftware durch private Akteure ist nur rechtswidrig, wenn diese Software in einem Verzeichnis verbotener Spähsoftware enthalten ist, das vom Leiter des EYP alle sechs Monate aktualisiert wird. Dies ermächtigt das EYP, Spähsoftware legal zu erwerben, da entsprechende kritische Sachverhalte ausschließlich über das Sekundärrecht (d. h. ein Präsidialdekret) behandelt werden. Daher wird eine aktualisierte Version der vorhandenen Spähsoftware als legal betrachtet, bis sie in das oben genannte Verzeichnis aufgenommen wird. Die Definition des Begriffs „nationale Sicherheit“ im Gesetz ist äußerst weit gefasst und vage und steht somit im Widerspruch zu Artikel 19 Absatz 1 der Verfassung, der eine enge Auslegung fordert. Die ADAE wird in ihren Bemühungen um die Ausübung ihrer verfassungsmäßig festgelegten Rolle bei der Kontrolle des Deklassifizierungsprozesses weiter behindert. Die Rolle der unabhängigen Behörde, die maßgeblich an der Aufdeckung des Überwachungsskandals

[279] https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022.
[280] https://www.dsa.gr/%CE%B4%CE%B5%CE%BB%CF%84%CE%AF%CE%B1-%CF%84%CF%8D%CF%80%CE%BF%CF%85/%CE%B1%CF%80%CE%BF%CF%86%CE%AC%CF%83%CE%B5%CE%B9%CF%82-%CE%B4%CF%83/%CE%B1%CF%80%CF%8C%CF%86%CE%B1%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%BF%CE%B9%CE%BA%CE%B7%CF%84%CE%B9%CE%BA%CE%BF%CF%8D-%CF%83%CF%85%CE%BC%CE%B2%CE%BF%CF%85%CE%BB%CE%AF%CE%BF%CF%85-%CF%84%CE%BF%CF%85-%CE%B4%CF%83%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7-%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B5%CE%B9%CF%83%CE%B1%CE%B3%CE%B3%CE%B5%CE%BB.
[281] Meinungsaustausch des PEGA-Ausschusses mit Konstantinos Menoudakos und Christos Rammos, 28. Februar 2023.

beteiligt war, rückt trotz der einschlägigen verfassungsrechtlichen Garantien im neuen Gesetz in den Hintergrund.

178. Die Möglichkeiten für Ex-post-Kontrollen wurden durch die Tatsache geschwächt, dass Griechenland lange gebraucht hat, um die Hinweisgeberrichtlinie der EU vollständig umzusetzen[282]. Am 27. Januar 2022 leitete die Kommission ein Vertragsverletzungsverfahren ein, indem sie Griechenland ein Mahnschreiben zukommen ließ. Am 15. Juli 2022[283] übermittelte die Kommission eine mit Gründen versehene Stellungnahme mit einer Beantwortungsfrist von zwei Monaten. Das griechische Parlament stimmte schließlich am 11. November 2022 über das Gesetz 4990/2022 ab, mit dem die Hinweisgeberrichtlinie der EU in griechisches Recht umgesetzt wurde.

ÖFFENTLICHE KONTROLLE

179. Griechenland belegt im World Press Freedom Index 2022 den letzten Platz unter allen EU-Ländern: d. h. Platz 108 von 180[284]. Im Jahr 2021 wurde der Journalist Giorgos Karaivaz ermordet. Der Mord wurde bis heute nicht aufgeklärt. Journalisten sind Einschüchterungen und taktischen Klagen gegen die öffentliche Beteiligung (SLAPP-Klagen) ausgesetzt. Grigoris Dimitriadis[285] hat SLAPP-Klagen gegen die Nachrichtenagenturen Reporters United und *Efimerida ton Syntakton* (EfSyn)[286] ein, nachdem er zum Rücktritt gezwungen wurde. Regierungsminister Oikonomou versuchte, die Politico-Reporterin Nektaria Stamouli zu diskreditieren, indem er ihr unterstellte, ihre Artikel über den Abhörskandal seien politisch motiviert[287]. In der Tat hatten zwei der Personen, die Opfer von Angriffen mit der Spähsoftware „Predator“ wurden, Koukakis und Malichoudis, kritisch über Korruptions- und Betrugsfälle und die Misshandlung von Migranten berichtet. Athanasios Telloglou und Eliza Triantafillou berichteten über den Spähsoftware-Skandal und wurden angeblich überwacht[288]. Darüber hinaus diskreditierte der oberste Staatsanwalt Griechenlands, Isidoros Dogiakos, Medien, die die griechischen Justizbehörden kritisierten, weil diesen den griechischen Abhörskandal nicht angemessen behandelten. Er versuchte sogar, die Medien, die den Skandal untersuchen, einzuschüchtern, indem er selektive Steuerprüfungen für ihre Eigentümer beantragte[289].

RECHTSBEHELF

NATIONALE TRANSPARENZBEHÖRDE

180. Wie in Artikel 82 des Gesetzes 4622/2019 festgelegt, ist die nationale Transparenzbehörde (EAD) dafür verantwortlich, die Rechenschaftspflicht, Transparenz

[282] https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768.
[283] https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768.
[284] https://rsf.org/en/index.
[285] Tagesspiegel.
[286] EUobserver, ‘Greece accused of undermining rule of law in wiretap scandal’.
[287] https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/
[288] Heinrich-Böll-Stiftung, ‘In conditions of absolute loneliness’.
[289] ESIEA Journalists Unions condemn threats from Supreme Court Prosecutor, https://www.esiea.gr/oi-dimosiografikes-enoseis-gia-tis-di/.

und Integrität der von Regierungsbehörden, staatlichen Institutionen, Verwaltungsbehörden und öffentlichen Organisationen durchgeführten Maßnahmen zu stärken. Darüber hinaus sollte der EAD Betrug und Korruption durch öffentliche und private Stellen verhindern, aufdecken und bekämpfen. Nach diesem Gesetz hat der EAD alle Verantwortlichkeiten, Rechte und Pflichten von folgenden öffentlichen Einrichtungen übernommen: dem Generalsekretariat für die Korruptionsbekämpfung; dem Gremium der Auditoren und Inspektoren der öffentlichen Verwaltung; dem Amt des Generalinspektors für öffentliche Verwaltung; dem Gremium der Inspektoren für Gesundheits- und Wohlfahrtsdienste; dem Gremium der Kontrolleure für öffentliche Arbeiten; und dem Gremium der Inspektoren und Prüfer des Verkehrs[290]. Während die Unabhängigkeit der ADAE in der Verfassung festgelegt ist, ist der EAD keine unabhängige Behörde.

181. Am 22. Juli 2022 leitete der EAD eine Untersuchung über den angeblichen Erwerb der Spähsoftware Predator durch das Ministerium für Bürgerschutz und das EYP ein. Bei der Prüfung wurden die griechische Polizei, der EYP und die Unternehmen Intellexa und Krikel überprüft. Der EAD schloss seinen Bericht am 10. Juli 2022 ab, gab ihn jedoch dem EYP zur vorherigen Genehmigung. Der offizielle Bericht, der Koukakis am 22. Juli übermittelt wurde, enthielt nur Bruchteile der vom EAD durchgeführten vollständigen Prüfung. Unter dem Deckmantel des Schutzes personenbezogener Daten wurden mehrere Namen im Prüfbericht geschwärzt, darunter die Namen der Prüfer des EAD, des Staatsanwalts des EYP, der den ursprünglichen EAD-Bericht überprüfte, sowie der Anwälte und Buchhalter der beteiligten juristischen Personen[291].

182. Der Bericht der nationalen Transparenzbehörde kam schließlich zu dem Schluss, dass weder der EYP noch das Ministerium für Bürgerschutz Verträge mit Intellexa und anderen verbundenen nationalen Unternehmen abgeschlossen hatten. Sie hätten auch die Spähsoftware „Predator“ nie erworben oder verwendet[292]. Die nationale Transparenzbehörde hat jedoch weder die Bankkonten von Intellexa und Krikel noch die angeschlossenen Offshore-Unternehmen untersucht. Darüber hinaus besuchte der EAD die Büros von Intellexa und Krikel erst zwei Monate, nachdem der Einsatz von Predator in Griechenland erstmals öffentlich wurde, als die Mitarbeiter aufgrund der COVID-19-Pandemie bereits von zu Hause aus arbeiteten. Die nationale Transparenzbehörde hat sich auch nicht mit den Rechtsvertretern der betreffenden Unternehmen getroffen[293].

183. Es gibt Zweifel an der Unabhängigkeit der Führung der nationalen Transparenzbehörde. Der derzeitige Direktor, ein ehemaliger Mitarbeiter von Mitsotakis, hat das Amt ad interim seit Sommer 2022 inne. Es ist unklar, warum das Einstellungsverfahren noch nicht begonnen hat. Der Direktor des EAD traf sich während der Informationsreise im November 2022 nicht mit PEGA. Der Direktor traf sich allerdings am 7. März 2023 mit der Delegation des LIBE-Ausschusses, wo Fragen zur Spähsoftware in Griechenland gestellt wurden.

[290] https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019
[291] Inside Story, ‘From Koukakis to Androulakis: A new twist in the Predator Spyware case’.
[292] Inside Story, ‘From Koukakis to Androulakis: A new twist in the Predator Spyware case’.
[293] Inside Story, ‘From Koukakis to Androulakis: A new twist in the Predator Spyware case’.

GRIECHISCHE BEHÖRDE FÜR KOMMUNIKATIONSSICHERHEIT UND DATENSCHUTZ (ADAE)

184. Im Juli 2022 bestätigte Nikos Androulakis, dass er bei der Staatsanwaltschaft des Obersten Gerichtshofs Anzeige erstattet hatte, weil er angeblich am 21. September 2021 mit der Spähsoftware „Predator“ ausgespäht worden war. Im Anschluss an Androulakis Beschwerde leitete die ADAE im August 2022 eine Untersuchung ein, in deren Rahmen zunächst Informationen von Androulakis Telekommunikationsanbieter eingeholt wurden.

185. Die Spähsoftware „Predator“ hinterlässt bei den Telekommunikationsanbietern wenige Spuren einer Infektion. Die ADAE stellte jedoch fest, dass das Mobiltelefon von Androulakis vom EYP überwacht wurde[294] und dass die Staatsanwältin des EYP, Vasiliki Vlachou, die Überwachungsmaßnahme und die Aufhebung der Vertraulichkeit im September 2021 genehmigt hatte, zeitgleich mit dem mutmaßlichen Predator-Angriff.

186. Auf die Untersuchungsergebnisse der ADAE hin traten Grigoris Dimitriadis und Panagiotis Kontoleon von ihren Regierungsämtern zurück[295]. Kontoleon erklärte, dass die Überwachung von Androulakis auf Ersuchen ausländischer Behörden – insbesondere der Geheimdienste Armeniens und der Ukraine – im Lichte der Beteiligung von Androulakis am Ausschuss für internationalen Handel des Europäischen Parlaments, der sich mit den Handelsbeziehungen zwischen der EU und China befasst, eingeleitet wurde[296]. Sowohl die Ukraine als auch Armenien bestritten diese Behauptungen[297].

187. Am 15. Dezember 2022 prüfte die Behörde auf Ersuchen des Journalisten Tasos Telloglou und des MdEP Giorgos Kyrtsos, ob sie vom EYP angegriffen worden waren. Eine Prüfung des Telekommunikationsunternehmens Cosmote durch die ADAE ergab, dass sowohl Telloglou als auch Kyrtsos tatsächlich überwacht wurden[298]. Cosmote informierte den Obersten Gerichtshof und stellte die Rechtmäßigkeit der Ermittlungen der ADAE in Frage[299]. Die ADAE richtete ein spezielles Team ein, um die Telekommunikationsanbieter zu prüfen, und suchte dabei insbesondere nach weiteren Anfragen des EYP zur Aufhebung der Vertraulichkeit[300].

188. Die Regierung hat versucht, die Mitglieder des Verwaltungsrats der ADAE zu ersetzen. Darüber hinaus gab der griechische Generalstaatsanwalt Dogiakos am 10. Januar 2023 offiziell eine Stellungnahme ab, in der er entschied, dass die ADAE keine Ermittlungen über die Aufzeichnungen von Telekommunikationsanbietern durchführen könne, um die Aufhebung der Vertraulichkeit der Kommunikation zu prüfen. Der Stellungnahme zufolge könnten strafrechtliche Sanktionen verhängt werden, sobald die ADAE solche

---

[294] https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf.
[295] Politico, ‘PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal’.
[296] https://www.kathimerini.gr/politics/561988786/ypothesi-parakoloythiseon-ta-dedomena-poy-pyrodotisan-tis-exelixeis/
[297] At a Glance, ‘Greece’s Predatorsgate: The latest chapter in Europe’s spyware scandal?’, European Parliament, Directorate-General for Parliamentary Research Services, 8 September 2022.
[298] Euractiv, ‘Exclusive: Another MEP and journalist the latest victims of “Greek Watergate”’.
[299] International Press Institute, ‘Greece: MFRR alarmed by latest revelations of spying on journalists’.
[300] Euractiv, ‘Exclusive: Another MEP and journalist the latest victims of “Greek Watergate”’.

Prüfungen einleitet[301]. Diese Stellungnahme, die früheren Meinungen des Generalstaatsanwalts widerspricht, verstößt eindeutig gegen die Unabhängigkeit der ADAE[302] und versucht, sie daran zu hindern, Ermittlungen durchzuführen. In einer Sitzung des PEGA-Ausschusses am 28. Februar 2023 erklärte Rammos, dass die Stellungnahme von Dogiakos nicht bindend sei und die Aufgaben der ADAE wie gewohnt fortgeführt werden könnten[303].

189. Die ADAE hat bestätigt, dass der EYP auch den Chef der griechischen Streitkräfte, Konstantinos Floros, einen amtierenden Minister, mehrere Amtsträger, die sich mit Waffenfällen befassen, und einen ehemaligen nationalen Sicherheitsberater ausspioniert hat. Da die ADAE derzeit nicht in der Lage ist, die Zielpersonen zu informieren, beabsichtigte sie, die Ergebnisse dem Transparenzausschuss des griechischen Parlaments und den Organen des griechischen Parlaments vorzulegen[304]. Christos Rammos schickte einen Brief an das griechische Parlament, in dem er um die Vorlegung dieser Ergebnisse bat. Zunächst vermied der Präsident es, das Thema zur Diskussion zu bringen, indem er sagte, dass er an seinem Namenstag keine Zeit gefunden habe, Rammos' Brief zu lesen. Schließlich lehnte die Néa-Dimokratía-Mehrheit im Ausschuss für Institutionen und Transparenz seinen Antrag ab. Am 24. Januar 2023 griff der Sprecher der Regierung die ADAE und ihren Präsidenten aufgrund ihrer Ermittlungen[305] an und behauptete, dass Rammos „Aktivismus" betreibe und sein Mandat „überschreite", was den Ermittlungen der ADAE nicht half. Am 25. Januar 2023 nannte der SYRIZA-Vorsitzende Alexis Tsipras öffentlich die Namen, die in dem Bericht des griechischen Parlaments aufgeführt sind, und bestätigte, dass der Leiter der Streitkräfte, der ehemalige Leiter der griechischen Armee, der Arbeitsminister, der nationale Sicherheitsberater des ehemaligen Premierministers sowie zwei Berater der Direktion für Ausrüstung der Streitkräfte vom EYP überwacht wurden. Im Hinblick auf den schwerwiegenden Charakter der Feststellungen stellt die Weigerung der ADAE, dem griechischen Parlament Bericht zu erstatten, und die Misskreditierung der Behörde eine Behinderung der Rechenschaftspflicht und Transparenz dar[306].

190. Darüber hinaus erklärte Rammos, dass die Änderungen am Rechtsrahmen der ADAE Unsicherheit geschaffen hätten, was zu einem Briefwechsel mit den Ministerien geführt habe, um den Handlungsrahmen der Behörde in Bezug auf Beschwerden und Untersuchungen zu klären. Rammos erwähnte, dass die ADAE etwa 10 Beschwerden

[301] Euractiv, 'Chief prosecutor puts Greece's rule of law to the test'.
[302]http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bdilosi-toy-proedroy-tis-adae-christoy-rammoy-gia-tin-g/.
[303] Meinungsaustausch des PEGA-Ausschusses mit Konstantinos Menoudakos und Christos Rammos, 28. Februar 2023.
[304]https://www.prototothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/.
[305]https://www.prototothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/.
[306]Newsbomb, ‚SYRIZA: Maximos circles" through ADAE – What he sees behind the "blockade" of ND in Rammos'.

pro Tag erhält[307].

AUSSCHUSS FÜR INSTITUTIONEN UND TRANSPARENZ

191. Im Juli 2022 lud der Ausschuss für Institutionen und Transparenz Kontoleon und den Präsidenten der ADAE, Christos Rammos, zu einer parlamentarischen Anhörung vor. Während dieser Anhörung räumte Kontoleon ein, dass das EYP Thanasis Koukakis aus Gründen der nationalen Sicherheit ausspioniert hatte, erklärte aber, dass er keine Kenntnis von dem versuchten Hacking-Angriff mit der Spähsoftware „Predator“ auf Androulakis’ Mobiltelefon hatte. Der Regierungssprecher Giannis Oikonomou erklärte, die griechischen Behörden hätten die Spähsoftware Predator weder erworben noch jemals eingesetzt[308].

192. Obwohl die Treffen unter Ausschluss der Öffentlichkeit[309]stattfanden, waren Berichten zufolge weder Kontoleon noch Dimitriadis bereit, substanzielle Beweise vorzulegen und beriefen sich dabei auf Gründe der nationalen Geheimhaltung[310]. Der neue Leiter des EYP, Demiris, verweigerte dem Ausschuss den Zugang zu einem Bericht mit Informationen über die angebliche Vernichtung von Überwachungsdaten[311]. Dies bedeutet effektiv, dass der EYP die Rechenschaftspflicht verweigert und das griechische Parlament sein Mandat der parlamentarischen Kontrolle nicht ausüben kann.

193. Am 30. August 2022 lud der Ausschuss neun Personen zu einer Anhörung hinter verschlossenen Türen vor, darunter die Staatsanwältin Vasiliki Vlachou, der ehemalige Generalsekretär Grigoris Dimitriadis und der ehemaliger Leiter des EYP, Kontoleon. Alle beriefen sich auf die Geheimhaltung vermieden es, während dieser Anhörung des Ausschusses Fragen zu beantworten[312].

PARLAMENTARISCHER UNTERSUCHUNGSAUSSCHUSS

194. Ein Vorschlag der PASOK-KINAL-Partei, einen Untersuchungsausschuss über den angeblichen Einsatz von Spähsoftware einzurichten,[313] wurde von 142 Oppositionsabgeordneten befürwortet, während sich die 157 Abgeordneten der Néa Dimokratía der Stimme enthielten[314]. Allerdings hatte die ND eine absolute Mehrheit im Untersuchungsausschuss. Die Forderungen nach einem überparteilichen Präsidium wurden abgelehnt. Die ND legte das Arbeitsprogramm und die Liste der vorzuladenden Zeugen fest und lehnte mehrere der von den Oppositionsparteien vorgeschlagenen Zeugen ab. Der Ausschuss wurde am 29. August 2022 eingesetzt. Er nahm seine Arbeit am 7. September 2022 auf und schloss sie am 10. Oktober 2022 ab.

---

[307]Meinungsaustausch des PEGA-Ausschusses mit Konstantinos Menoudakos und Christos Rammos, 28. Februar 2023.
[308] Reuters. Greek intelligence service admits spying on journalist - sources.
[309] Ekathimerini, ‘Transparency committee to hold closed-door meeting on phone hacking allegation’.
[310] Tovima, ‘In combat positions for eavesdropping’.
[311] Tovima, ‘In combat positions for eavesdropping’.
[312] Ieidiseis, ‘SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up’, https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi.
[313] Tovina. Interceptions: Committee of Inquiry to monitor Androulakis - Pasok’s proposal in detail.
[314] Tovina. *Parliament: The 2016 inquiry into surveillance was passed - with 142 votes in favour.*

195. Die Regierungsmehrheit im Ausschuss weigerte sich, Bitzios und Lavranos vorzuladen. Stattdessen erfolgte die Vorladung von Stamatis Tribalis – dem derzeitigen Geschäftsführer von Krikel – und Sara Hamou. Am 22. September sagte Tribalis vor diesem parlamentarischen Ausschuss aus. Tribalis legte offenkundig falsche Informationen über die Beteiligung von Bitzios und Lavranos an Krikel vor und behauptete unter anderem, er selbst sei der Eigentümer von Krikel[315].

196. Eine Zeugin, Sara Hamou, die für das Unternehmen Intelexa tätig ist, gab an, nicht persönlich erscheinen zu können (obwohl sie in Zypern lebt), und es wurde ihr gestattet, ihre Antworten schriftlich einzureichen. Gemeinsame Schlussfolgerungen konnten aufgrund einer starken Polarisierung der politischen Landschaft nicht erzielt werden. Eine von der Regierung geführte Mehrheit beschloss, etwa 5 500 Seiten an Dokumenten als Verschlusssache einzustufen, einschließlich der Protokolle und der Aussage von Hamou, wurden als Verschlusssache eingestuft, obwohl es in der Macht des Parlaments liegt, diese unter Verschluss zu halten oder freizugeben. Daher wurde keine öffentliche Zusammenfassung erstellt. Nur die abschließende Aussprache im Plenum des griechischen Parlaments war öffentlich und sowohl die Ergebnisse von PASOK als auch von SYRIZA wurden von den Parteien selbst veröffentlicht.

197. Die Opposition schlug andere Zeugen vor, wie Koukakis, Mitsotakis, Dimitriadis, Vlachou, Lavranos und Bitzios, aber der Ausschuss lehnte es schließlich ab, sie vorzuladen. Am 10. Oktober 2022 beendete der Ausschuss seine Untersuchungen und die verschiedenen politischen Parteien legten alle ihre Abschlussberichte vor[316].

GRIECHISCHE DATENSCHUTZBEHÖRDE

198. Die Griechische Datenschutzbehörde (HDPA) ist eine unabhängige Behörde und hat die Aufgabe, die Anwendung der Datenschutz-Grundverordnung[317] (DSGVO) sowie anderer Vorschriften und nationaler Gesetze zum Datenschutz von Personen in Griechenland zu überwachen[318]. Seit dem Gesetz von 1997 fiel die nationale Sicherheit in den Zuständigkeitsbereich der HDPA, doch das Gesetz 4624/2019 schloss sie davon aus[319]. Nach der Beschwerde von Nikos Androulakis im Juli 2022 leitete die Behörde im Juli 2022 eine Untersuchung über die Installation von Spähsoftware auf Mobiltelefonen und die anschließende Erhebung und Verarbeitung personenbezogener Daten ein. Die Behörde führte eine Prüfung im Büro von Intellexa in Chalandri und in einer Einrichtung von Intellexa in Elliniko durch. Intellexa lieferte jedoch keine wesentlichen Informationen und beantwortete die Fragebögen erst nach erheblicher Verzögerung, was die Prüfung der Behörde behinderte[320].

---

315 TVXS. *G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament*.
316 Ieidiseis. *SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up*.
317 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4.5.2016, S. 1).
318 Griechische Datenschutzbehörde. *Personal data*.
319 Government Gazette of the Hellenic Republic.
320 Griechische Datenschutzbehörde. Verhängung einer Geldbuße gegen Intellexa S.A. wegen mangelnder Bereitschaft zur Zusammenarbeit mit der HDPA.

199. Am 16. Januar 2023 verhängte die HDPA eine Geldbuße von 50 000 EUR gegen[321] Intellexa S.A. wegen ihrer Behinderung der Arbeiten und ihrer mangelnden Bereitschaft zur Zusammenarbeit bei der Prüfung auf der Grundlage von Artikel 31 DSGVO.

200. Nach den Maßnahmen der HDPA hat Intellexa Dokumente eingereicht, aber die Behörde prüft sie immer noch. Laut dem Präsidenten der HDPA, Herrn Menoudakos, habe die Behörde Domainnamen entdeckt, die möglicherweise zu Unternehmen gehören, die innerhalb und außerhalb der EU mit Intellexa zusammenarbeiten. Die Untersuchung der HDPA ist noch nicht abgeschlossen[322].

201. In einer Sitzung des PEGA-Ausschusses am 28. Februar 2023 erwähnte der Vorsitzende der HDPA, dass eine HDPA-Untersuchung Internetapplikationen für das Versenden von Textnachrichten untersucht habe. Laut Herrn Menoudakos haben Unternehmen diese Internetanwendungen genutzt, um Textnachrichten im Zusammenhang mit der Spähsoftware „Predator“ zu liefern. Die HDPA versucht derzeit, die Zielpersonen zu identifizieren, hat aber bisher bestätigt, dass mit dieser Methode 300 Textnachrichten an etwa 100 Empfänger gesendet wurden. Die HDPA hat die Unternehmen angewiesen, diese Daten zu speichern, und betont, dass diese Unternehmen, wenn sie keinen gesetzlichen Vertreter in der EU haben, gegen die DSGVO verstoßen[323].

DIE ZIELE

THANASIS KOUKAKIS

202. Im Sommer 2020 wurde der Journalist Thanasis Koukakis vom EYP abgehört. Zu dieser Zeit berichtete er über Finanzthemen, einschließlich des Piräus/Libra-Skandals, in den Felix Bitzios verwickelt war, über die angebliche Steuerhinterziehung durch den griechischen Geschäftsmann Yiannis Lavranos sowie über die umstrittenen Bankengesetze, die von der Regierung Mitsotakis eingeführt wurden und die die Verfolgung von Geldwäsche und anderen Finanzdelikten behinderten (tatsächlich hatten die neuen Vorschriften rückwirkend die Einstellung von zwölf anhängigen Verfahren zur Folge)[324]. Koukakis untersuchte auch die Beschaffung neuer Personalausweise, an denen Lavranos und Bitzios ein geschäftliches Interesse hatten. Etwa zu der Zeit, als Koukakis zum ersten Mal vor dem PEGA erschien, wurde die Ausschreibung plötzlich zurückgezogen und der zuständige Generalsekretär trat zurück.

203. Am 29. Juli 2022 erklärte der EYP-Chef Panagiotis Kontoleon, dass das EYP das Telefon von Herrn Koukakis aus „Gründen der nationalen Sicherheit“ überwacht habe.

204. Am 1. Juni 2020 stellte der EYP einen ersten Antrag auf Aufhebung der Vertraulichkeit der Telefonnummer von Herrn Koukakis für zwei Monate bis zum 1. August 2020. Der

[321] Griechische Datenschutzbehörde. Verhängung einer Geldbuße gegen Intellexa S.A. wegen mangelnder Bereitschaft zur Zusammenarbeit mit der HDPA.
[322] Meinungsaustausch des PEGA-Ausschusses mit Konstantinos Menoudakos und Christos Rammos. 28.02.2023.
[323] Meinungsaustausch des PEGA-Ausschusses mit Konstantinos Menoudakos und Christos Rammos. 28.02.2023.
[324] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?*.

EYP beantragte eine Verlängerung um weitere zwei Monate, d. h.[325]bis zum 1. Oktober 2020. Die Staatsanwältin des Berufungsgerichts – Vasiliki Vlachou – hat all diese Bestimmungen aus Gründen der nationalen Sicherheit genehmigt[326].

205. Zwölf Tage später, am 12. August 2020, beantragte der EYP jedoch plötzlich die Aufhebung der Geheimhaltung der Telefonnummer von Herrn Koukakis, d. h. anderthalb Monate früher als im ursprünglichen Antrag vorgesehen. Dies geschah am selben Tag, als Koukakis sich an die ADAE wandte, um über die mögliche Überwachung seiner beiden Mobiltelefone und eines Festnetztelefons informiert zu werden.

206. Am 10. März 2021 informierte die ADAE den Staatsanwalt des EYP über die Möglichkeit, Koukakis über die Überwachung seines Mobiltelefons zu benachrichtigen. Am 31. März verabschiedete die griechische Regierung jedoch die Gesetzesänderung 826/145, mit dem die ADAE der Fähigkeit beraubt wurde, Bürger rückwirkend über die Aufhebung der Vertraulichkeit ihrer Kommunikation zu informieren[327]. Der Präsident der ADAE, Christos Rammos, und zwei weitere Mitglieder der ADAE haben sich gegen diese Gesetzesänderung ausgesprochen und in einer Stellungnahme darauf hingewiesen, dass die Gesetzesänderung das in der Europäischen Menschenrechtskonvention (EMRK) verankerte Recht auf Achtung des Privat- und Familienlebens und den in der Verfassung garantierten Schutz der Vertraulichkeit der Kommunikation verletzt[328].

207. Zwischen dem 12. Juli 2021 und dem 14. September 2021 war das Telefon von Herrn Koukakis mit der Spähsoftware Predator infiziert[329]. Laut Herrn Koukakis erhielt er eine SMS mit einem Link zu einer Finanznachrichten-Webseite[330]. Am 28. März 2022 deckte Citizen Lab offiziell die Infektion auf[331].

208. Herr Koukakis unternahm mehrere Versuche, Rechtsbehelf gegen die Überwachungsversuche zu erhalten. Er reichte zwei Beschwerden bei der ADAE ein: die erste am 6. April 2022, bei der er eine gründliche Untersuchung seines Mobiltelefons auf eine Infektion mit Predator beantragte; die zweite am 13. Mai 2022 im Lichte der neuen Enthüllungen von InsideStory und Reporters United. Darüber hinaus reichte Herr Koukakis am 4. Mai 2022 beim EAD eine Beschwerde ein, in der er eine Untersuchung des Hintergrunds der Abhörmaßnahmen des EYP und des Predator-Angriffs beantragte[332].

---

[325] Reporter United. *Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*.
[326] Reporters United. *Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*; Inside Story. *Who was tracking journalist Thanasis Koukakis' cell phone?*.
[327] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis: https://www.reportersunited.gr/8646/eyp-koukakis/ Inside Story. Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?*.
[328] Constitutionalism. Contradiction of Article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications: https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/.
[329] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?*.
[330] Europäisches Parlament. Anhörung vom 8. September 2022.
[331] Inside Story. *Who was tracking journalist Thanasis Koukakis' cell phone?*.
[332] Avgi. *Thanasis Koukakis / Filed a lawsuit for the Predator – Who and why was watching him.*

209. Die Untersuchung der EAD vom 21. Juli 2022 in den Athener Büros von Intellexa, dem Anbieter von Predator, war begrenzt und oberflächlich, trotz der Tatsache, dass wichtige Informationen über die Angriffe mit Predator – eine Straftat – hätten entdeckt werden können. Es wurden keine Server, IT-Hardware oder -Administration beschlagnahmt und sichergestellt. Die Überprüfung der Finanzverwaltung beschränkte sich auf das Jahr 2020[333]. Die Tochtergesellschaften von Intellexa in Zypern und Irland wurden überhaupt nicht untersucht[334]. Die Ermittlungen enthielten keine Informationen über die Bankkonten von Intellexa und ihren Tochtergesellschaften[335]. Herr Koukakis legte am 27. Juli 2022 Berufung beim Europäischen Gerichtshof für Menschenrechte ein[336].

210. Am 5. Oktober 2022 legte Herr Koukakis eine Beschwerde bei der Staatsanwaltschaft in Athen gegen Intellexa Alliance, insbesondere gegen Tal Dilian und Sara Hamou[337], wegen Verletzung der Vertraulichkeit seiner Kommunikation ein[338].

NIKOS ANDROULAKIS

211. Am 21. September 2021 wurde Nikos Androulakis, Vorsitzender der Mitte-Links-Partei PASOK-KINAL und Mitglied des Europäischen Parlaments, mit der Spähsoftware „Predator“ angegriffen, als er einen bösartigen Link auf seinem Telefon zugeschickt bekam[339]. Androulakis erhielt eine Textnachricht mit dem Wortlaut „Machen Sie mal ein bisschen Ernst, wir haben viel zu gewinnen“. Außerdem enthielt die Nachricht einen Link zur Installation der Spähsoftware „Predator“ auf seinem Telefon. Im Gegensatz zu Koukakis klickte Androulakis jedoch nicht auf den Link, der ihm zugesandt wurde[340]. In einer Sitzung des PEGA-Ausschusses am 28. Februar 2023 sagte Herr Androulakis aus, dass die HDPA das Kreditkartenkonto identifiziert habe, das für die ihm übermittelten SMS bezahlt habe. Diese Informationen wurden an die zuständige Staatsanwaltschaft weitergegeben[341].

212. Im Juli 2021 kündigte Herr Androulakis seine Kandidatur für die Parteiführung an[342]. Laut der Untersuchung der ADAE wurde das Mobiltelefon von Herrn Androulakis damals vom EYP über die Telekommunikationsanbieter überwacht[343]. Die Staatsanwältin des EYP, Vasiliki Vlachou, genehmigte die Aufhebung der Vertraulichkeit des Telefons von Herrn Androulakis aus Gründen der nationalen Sicherheit. Die Genehmigung fiel sowohl mit dem Predator-Angriff als auch mit der Kandidatur von Herrn Androulakis zusammen.

213. Als Herr Androulakis im Dezember 2021 zum Parteivorsitzenden gewählt wurde, wurde

---

[333] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[334] InsideStory. *From Koukakis to Androulakis:* A new twist in the Predator spyware case.
[335] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[336] BBC. *Greece wiretap and spyware claims circle around PM Mitsotakis.*
[337] News 24 7. Wiretapping scandal: Lawsuit against Intellexa by Thanasis Koukakis.
[338] Heinrich Boll Stiftung. *A State of Absolute Solitude*.
[339] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[340] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader*.
[341] Meinungsaustausch des PEGA-Ausschusses mit Konstantinos Menoudakos und Christos Rammos. 28.02.2023.
[342] Tovima. Androulakis lashes out at PM, ND spokesman says Pasok leader should say why his phone was tapped.
[343] Kathimerini. *Surveillance case: the data that triggered the developments*.

die „offizielle“ EYP-Überwachung abrupt eingestellt[344], obwohl die Verlängerung der Genehmigung für seine Überwachung um zwei weitere Monate noch nicht abgelaufen war.

214. Am 28. Juni 2022 prüfte die GD ITEC des Europäischen Parlaments das Telefon von Herrn Androulakis und fand die Beweise für den versuchten Predator-Hackingangriff vom September 2021, über den sie Herrn Androulakis unterrichtete[345]. Herr Androulakis erhob am 26. Juli 2022 Klage bei der Staatsanwaltschaft des Obersten Gerichtshofs[346].

215. Wenige Tage später, am 29. Juli, legte Herr Androulakis der ADAE die Informationen über den Predator-Angriff vor. Am selben Tag hörten der Ständige Ausschuss für Institutionen und Transparenz den EYP-Chef Panagiotis Kontoleon und Christos Rammos, den Präsidenten der ADAE, in Anwesenheit des Ministers für Digitale Governance und dem Staatsminister an. Das Treffen fand hinter verschlossenen Türen statt[347].

216. Am 8. September 2022 bat Herr Androulakis die ADAE, ihm seine Abhördateien zu übermitteln[348]. Am selben Tag berichtete die Tageszeitung Ta Nea jedoch über eine offizielle Einweisung der ADAE, in der erwähnt wurde, dass sowohl die Akten von Herrn Androulakis als auch die von Herrn Koukakis vom EYP vernichtet worden seien[349]. Die Vernichtung ist eine eindeutige Tatsache, die Geschichte dahinter bleibt jedoch unklar. Einerseits sehen einige Quellen die Ursache für die Vernichtung der Dateien in einer Umstellung der elektronischen Systeme des EYP im Jahr 2021[350]. Durch diese Umstellung auf das neue juristische Datenbanksystem wurde angeblich ein technisches Problem verursacht, das zur Vernichtung führte. Auf der anderen Seite behaupten andere Quellen, dass Herr Kontoleon am 29. Juli 2022 den Befehl erteilt habe, diese Akten am selben Tag zu vernichten, an dem Androulakis die ADAE über die Überwachungsversuche informierte[351]. Während einer Anhörung des PEGA-Ausschusses hat der Präsident der ADAE, Herr Rammos, die Vernichtung von Aufzeichnungen weder bestätigt noch bestritten[352].

217. Am 5. August traten die Herren Kontoleon und Dimitriadis von ihren Ämtern zurück. Am 8. August gab Herr Mitsotakis im Fernsehen eine Erklärung ab, in der er zwar einräumte, dass Herr Androulakis abgehört worden sei, aber erneut darauf verwies, dass er davon nichts gewusst habe[353].

218. Der EYP hat sich bisher geweigert, die Gründe für die Überwachung offenzulegen. Er hat angeboten, Herrn Androulakis privat über die Gründe zu informieren. Das wäre rechtswidrig. Herr Androulakis bat darum, dass seine Überwachungsakte dem

---

[344] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader.*
[345] Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.
[346] News 247. Nikos Androulakis: Near-Victim of Predator Software - Filed a Lawsuit.
[347] Avgi. *Predator scandal / EYP dragged to Parliament over surveillance.*
[348] Ekathimerini. Androulakis asks ADAE for his wiretapping file.
[349] TaNea*. The archive of the surveillance of Nikos Androulakis destroyed.*
[350] TVXS. *G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.*
[351] Ieidiseis*. SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.*
[352] European Parliament. Sitzung am 8. September 2022.
[353] Reuters*. Greek PM says he was unaware of phone tapping of opposition party leader.*

Ausschuss für Institutionen und Transparenz vorgelegt wird, was jedoch abgelehnt wurde.

219. Am 7. Dezember 2022 legte Herr Androulakis wegen seiner Abhörung durch den EYP und das Fehlen offizieller Informationen über seinen Fall Beschwerde beim Europäischen Gerichtshof für Menschenrechte ein[354].

220. Die Überwachung eines Politikers ist höchst ungewöhnlich, und die griechische Verfassung sieht einen besonderen Schutz der Politiker vor. Der EYP bestreitet jede Beteiligung an der Überwachung mit der Spähsoftware „Predator“. Die Regierung hat zunächst Vermutungen über die Involvierung ausländischer Mächte geäußert, die angeblich die Überwachung von Herr Androulakis beantragt hätten, oder stellte in den Raum, seine Mitgliedschaft in einem Ausschuss des Europäischen Parlaments, der für die Beziehungen zu China zuständig ist, könnte ihn zur Zielscheibe gemacht haben. Keine dieser Hypothesen war besonders glaubwürdig. Die Überwachung fand in einem politischen Kontext statt, kurz vor den Wahlen. Die PASOK würde bei den Wahlen als der bevorzugte Koalitionspartner hervorgehen. Im Herbst 2021 traten vier Kandidaten für die Führung der PASOK an, die jeweils unterschiedliche Ansichten über eine solche Koalition hatten. Herr Androulakis hieß es, er sei offen für die Idee, aber nicht unter der Premierministerschaft von Herrn Mitsotakis. Ein anderer Kandidat, Andreas Loverdos, hatte zuvor als Minister in einer Koalition aus Néa Demokratía und PASOK gedient und galt eher als Befürworter der Idee. Er war mit Herrn Dimitriadis bekannt. Angesichts der Liste weiterer angeblicher Zielpersonen, die durch Documento veröffentlicht wurde, erhärtet sich der Verdacht, dass die Überwachung politisch motiviert war. Es gibt keine Beweise für eine dieser Hypothesen, aber es ist wichtig, dass diese untersucht und nach Möglichkeit aus der Welt geräumt werden.

GIORGOS KYRTSOS

221. Am 15. Dezember 2022 wurde bei einer Prüfung des Telekommunikationsunternehmens Cosmote durch die ADAE bestätigt, dass das Mitglied des Europäischen Parlaments Giorgos Kyrtsos vom EYP überwacht wurde[355]. Sowohl seine Mobiltelefone als auch sein Festnetz wurden abgehört. Die Überwachung wurde Berichten zufolge neun[356] Mal um einen Zeitraum von 18 Monaten verlängert.

222. Giorgios Kyrtsos ist ein ehemaliges Mitglied der Nea Demokratia und der Europäischen Volkspartei. Im Februar 2022 wurde Herr Kyrtsos von der ND aus der griechischen Regierungspartei ausgeschlossen, weil er das Vorgehen der Regierung im Zusammenhang mit der COVID-19-Pandemie, Beschränkungen der Medienfreiheit und den Umgang mit dem Novartis-Skandal missbilligte[357]. Nach seinem Ausschluss trag Herr Kyrtsos Renew Europe bei.

STAVROS MALICHOUDIS

223. Am 13. November 2021 enthüllte die Zeitung EFSYN, dass mehrere Journalisten, die

[354] Ekathimerini. *Socialist leader appeals to European Court over tapping.*
[355] Euractiv. *Another MEP and journalist the latest victims of ‘Greek Watergate’.*
[356] Politico. *Greek prosecutor slams unflattering comparisons to Belgium’s Qatargate probe.*
[357] Euractiv. *Renew Europe welcomes first Greek MEP who left PPE.*

über Flüchtlingsfälle berichteten, angeblich von der EYP abgehört wurden. Ein internes Dokument des EYP zeigte, dass der EYP die Überwachung und Sammlung von Daten des griechischen Journalisten Stavros Malichoudis angeordnet hatte[358][359]. Malichoudis schrieb über ein 12-jähriges syrisches Kind, das mehrere Monate in einem Internierungslager auf der griechischen Insel Kos leben musste[360].

224. Am 15. November 2021 bestätigte der Regierungssprecher Giannis Oikonomou indirekt diese Behauptungen. Er erklärte, dass der EYP Personen abhören könne, wenn ein Risiko für die nationale Sicherheit durch interne oder externe Bedrohungen bestehe[361]. Am 24. November und am 17. Dezember 2021 dementierte Staatsminister George Gerapetritis jedoch, dass Journalisten in Griechenland, darunter Herr Malichoudis, überwacht worden seien, doch dem Medienunternehmen Solomon zufolge hat er die Echtheit der internen EYP-Dokumente weder bestätigt noch bestritten[362].

225. Während der PEGA-Anhörung zu Griechenland am 8. September 2022 erklärte Herr Malichoudis, dass der EYP durch das Abhören seines Telefons auch Informationen von Kollegen und Journalisten sammeln konnte, mit denen er in dieser Zeit in Kontakt stand[363]. Der EYP hätte angeblich Gespräche von Herrn Malichoudis mit der Internationalen Organisation für Migration (IOM)[364] mithören können, wobei er auf die Gefahren verwies, die für andere, den sogenannten Beifang des Abhörens, entstehen würden. Während der Anhörung legte Herr Malichoudis außerdem Beweise dafür vor, dass der EYP an seiner Arbeit und seinen Quellen interessiert gewesen sei, der Grund für die Überwachung jedoch von der nationalen Sicherheit abgedeckt sei[365].

CHRISTOS SPIRTZIS

226. Am 9. September 2022 wurde der ehemalige Minister für Infrastruktur und Abgeordnete der Syriza-Partei Christos Spirtzis nach eigener Aussage mit der Spionagesoftware Predator auf seinem Mobiltelefon angegriffen[366]. Spirtzis hatte der Regierung am 15. November 2021 kritische parlamentarische Anfragen zu den Überwachungsaufgaben des EYP vorgelegt. Am selben Tag erhielt er eine ähnliche Botschaft[367] wie Nikos Androulakis. Am 19. November wurde eine zweite Nachricht an Christos Spirtzis gesandt, die einen Link zu einem Artikel von Efimerida ton Syntakton enthielt[368]. Während CitizenLab diese Nachrichten nicht überprüfte, teilte Spirtzis die Links, die er erhielt, mit zwei Technikern, die mündlich bestätigten, dass er angegriffen worden war.[369] Am 9. September 2022 legte Spirtzis beim Staatsanwalt des Obersten

[358] Efsyn. *Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ.*
[359] Solomon. *Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'*.
[360] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*
[361] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*
[362] Solomon, *Solomon's* reporter *Malichudos* under surveillance for national security reasons.
[363] European Parliament. Sitzung am 8. September 2022.
[364] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*
[365] European Parliament. Sitzung am 8. September 2022.
[366] Ekathimerini. Former SYRIZA minister says he was targeted by Predator.
[367] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware.*
[368] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware. („Hacking-Versuch bei Christos Spirtzis, MP für die Opposition, mit illegaler Predator-Spähsoftware.")*
[369] Inside story, *Predator: More than 20 targets in Greece according to the Data Protection Authority.*

Gerichtshofs Beschwerde ein[370]. Spirtzis ist ein Vertrauter des Parteichefs Alexis Tsipras, der bei hochrangigen Treffen der Parteiführung anwesend ist.

TASOS TELLOGLOU, ELIZA TRIANTAFYLLOU UND THODORIS CHONDROGIANNOS

227. Die Journalisten Tasos Telloglou und Eliza Triantafylou wurden angeblich bespitzelt, während sie investigativ für das neue Magazin „Inside Story" tätig waren. In einem Artikel für die Heinrich Böll-Stiftung vom 24. Oktober 2022 berichtete Telloglou über seine Überwachungs- und Einschüchterungserfahrungen bei der Untersuchung der Überwachungsskandale in Griechenland. Nach diesen Erfahrungen glaubt er, dass er zwischen Mai und August 2022 überwacht wurde[371].

228. Außerdem hat eine Quelle aus den Sicherheitsdiensten im Juni 2022 Telleglou berichtet, dass sowohl sein Wohnsitz als auch der seiner Kollegen Eliza Triantafyllou (InsideStory) und Thodoris Chondrogiannos (Reporters United) von den Behörden überwacht würden, um herauszufinden, mit welchen Quellen sie sich treffen würden[372]. Zum Zeitpunkt der Erstellung dieses Berichts hat die griechische Regierung noch nicht auf die Vorwürfe reagiert.

229. Am 15. Dezember 2022 wurde bei einer Prüfung des Telekommunikationsunternehmens Cosmote durch die ADAE bestätigt, dass Telloglou vom EYP überwacht wurde. Aufgrund der „nationalen Sicherheit" wurden die Gründe für die Überwachung nicht offengelegt[373].

SONSTIGE ZIELPERSONEN

230. Am 29. Oktober 2022 wurde berichtet, dass auch andere Politiker mit der Spähsoftware „Predator" ausspioniert wurden, darunter ein Minister der Regierung, der in keinem guten Verhältnis zum Premierminister stand. Darüber hinaus soll ein weiteres Mitglied der Néa Demokratía einen Link für die Installation der Spähsoftware „Predator" erhalten haben[374]. Ein Regierungssprecher, Herr Oikonomou, ließ verlautbaren, dass sich der Artikel auf keinerlei konkreten Beweise stütze[375].

231. Am 5. und 6. November 2022 veröffentlichte Documento eine Liste mit 33 Namen von Personen, die mithilfe der Spähsoftware „Predator" ausgespäht wurden[376]. Die Liste umfasste viele hochrangige Politiker, unter anderem auch Mitglieder der aktuellen Regierung, der ehemalige Premierminister Samaras, der ehemalige EU-Kommissar Avramopoulos, der Chefredakteur einer regierungsfreundlichen nationalen Zeitung und Personen aus dem Umfeld von Vangelis Marinakis, Reeder, Medienmogul und Besitzer

---

[370] Reuters. *One more Greek lawmaker files complaint over attempted phone hacking; Euractiv. Zweiter griechischer Oppositionsabgeordneter Opfer von Abhöraffäre*
[371] Heinrich-Böll-Stiftung. *A State of Absolute Solitude*.
[372] MapMF, *Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations.*
[373] Euractiv, Another MEP and journalist the latest victims of 'Greek Watergate'.
[374] Ta Nea, *Four illegal manipulations by suspicious center. („Vier illegale Manipulationen durch verdächtiges Zentrum.")*
[375] Politico, *Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes. („Lula siegt in Brasilien – Süßes oder Handel – Probleme beim Getreidehandel.")*
[376] Documento, 6. November 2022.

der Fußballclubs Olympiakos und Nottingham Forest. Die ADAE bestätigte, dass einige Namen auf der Liste vom EYP durch konventionelle Telefonüberwachung abgehört wurden. Zu diesen Namen gehören MdEP Giorgos Kyrtsos[377], Generalstabschef General Konstantinos Floros[378], Chef der griechischen Landstreitkräfte Haralambos Lalousis[379], Minister für Arbeit und Soziales Kostis Hatzidakis[380], die ehemaligen Generaldirektoren für Verteidigungsausrüstung und Investitionen Theodoros Lagios und Aristides Alexopoulos[381], der ehemalige Sicherheitsberater Alexandros Diakopoulos[382] und der griechische Investigativjournalist Tasos Telloglou[383].

232. Zudem war auch die ehemalige Cybersecurity Policy Manager von Meta, Artemis Seaford, einer der 33 Namen. Es wurde bestätigt, dass sie gleichzeitig vom EYP abgehört und mit Predator ausgespäht wurde. Seaford wurde vom EYP von Juli 2021 bis zum Sommer 2022 abgehört. Das heißt, dass die Genehmigung für das Abhören des Geräts von Frau Seaford sechs Mal verlängert wurde, was im Prinzip die Genehmigung des hauseigenen Staatsanwalts des EYP, Vasiliki Vlachou, erfordert. CitizenLab bestätigte, dass ihr Mobiltelefon seit September 2021 auch für mindestens zwei Monate mit Predator infiziert war. Die Predator-Infektion ereignete sich damit etwa ein bis zwei Monate nach Beginn des konventionellen Abhörens. Laut Frau Seaford wurden Informationen über ihren Termin für eine COVID-19-Impfung mittels konventionellem Abhören aus ihren Textnachrichten erlangt. Anhand dieser Informationen wurde anschließend eine ausgefeilte automatisierte SMS mit der gleichen Aufmachung wie der offizielle Termin erstellt, mit der Bitte, den Termin über einen Link zu bestätigen. Durch Klicken auf diesen Link wurde das Gerät mit der Predator-Spähsoftware infiziert. Die SMS-Nachricht enthielt genaue und detaillierte Informationen über ihre Impfdatei, und sie wurde mit einem Abstand von nur wenigen Minuten von den echten, offiziellen Nachrichten gesendet. Das deutet darauf hin, dass die Person, die die Nachrichten gesendet hat, Zugriff auf den Inhalt und das Timing der SMS-Nachrichten hatte. Dies wäre dem EYP durch den herkömmlichen Abhörvorgang möglich gewesen.

233. Das Abhören und/oder die Überwachung einer Privatperson ist ungewöhnlich, insbesondere wenn die nationale Sicherheit in einem solchen Fall nicht rechtmäßig geltend gemacht werden kann. Dies wirft die Frage auf, welche anderen Motive beim Targeting eine Rolle gespielt haben könnten. Die Überwachung erfolgte, als Frau Seaford bei Meta tätig war, ein Unternehmen, das einen Threat Report on the Surveillance-for-Hire Industry („Bericht über die Auftragsüberwachungsindustrie) veröffentlicht und mehrere Spähsoftware-Unternehmen, darunter Cytrox, von seiner Plattform verbannt hat. Es ist jedoch äußerst unwahrscheinlich, dass ihre Funktion bei Meta der Grund für die Überwachung war. Der Meta-Bericht wurde erst im Dezember

---

[377] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*.
[378] https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyp-toy-mitsotakiAvgi,
[379] *https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyp-toy-mitsotaki*.
[380] https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/.
[381] *https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/*.
[382] *https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/*.
[383] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*.

2021 veröffentlicht, einige Monate nach dem Angriff auf das Gerät von Frau Seaford. Außerdem wurde keine der anderen Personen, die an der Erstellung des Berichts beteiligt waren, selbst ins Visier genommen. Darüber hinaus erklärte Frau Seaford,[384] dass sie nur teilweise an diesen Aktivitäten beteiligt gewesen sei und dass Meta bei der Nennung der Namen seiner Beschäftigten äußerst diskret vorgehe.

234. Im März 2021 veröffentlichte das Magazin Marie-Claire einen Artikel mit einem Auszug aus einer Buchreihe von Frau Seaford. Der Artikel erwähnt Seafords Erfahrungen mit alltäglichem Sexismus und Belästigung in Griechenland und beschreibt insbesondere einen Fall sexueller Belästigung durch ‚einen Politiker'[385]. Die Überwachung begann einige Monate später. Eine Erklärung könnte sein, dass der betreffende Politiker den Artikel las und befürchtete, dass sein Name öffentlich bekannt werden könnte. Eine andere Erklärung könnte sein, dass jemand anderes den Politiker aus der Beschreibung im Artikel erkannte und aus politischen Gründen mehr Informationen über diese Person sammeln wollte. Unabhängig davon, was tatsächlich dahintersteckte, hätten nur sehr wenige Personen die Befugnis, sowohl einen offiziellen Antrag auf Abhörung beim EYP zu stellen, als auch die Verwendung von Predator-Spähsoftware zu veranlassen. Die Kombination aus Überwachung durch den EYP und Predator-Spähsoftware wurde auch in anderen Fällen bestätigt.

235. Es ist wichtig, dass diese Möglichkeiten weiter untersucht werden, insbesondere die Frage, wer die Überwachung durch das EYP beantragt hat. Frau Seaford hat bei der ADAE einen entsprechenden Antrag gestellt und beim griechischen Gericht Beschwerde eingelegt. Die Ermittlungen sind jedoch noch im Gange. Sie ist die erste amerikanische Staatsbürgerin, die in der EU Opfer eines solchen Angriffs wurde[386][387].

236. Andere Namen auf der Liste, die nicht offiziell bestätigt wurden, sind der ehemalige Minister für Bildung und Kultusfragen Andreas Loverdos, der ehemalige Ministerpräsident Antonis Samaras, der Staatsminister George Gerapetritis, das ehemalige Mitglied der Kommission Dimitris Avramopoulos, der Minister Nikos Dendias, der Bildungsminister Niki Kerameus, der Minister Akis Skertsos, der Investitionsminister Nikos Papathanasis, der ehemaliger Bürgerschutzminister Mihalis Chrysochoidis, der stellvertretender Verteidigungsminister der Hellenischen Republik Nikos Hardalias, Aristotelia Peloni, der Abgeordneter Christos Spirtzis, die ehemalige Bürgerschutzministerin Olga Gerovasili, der Leiter der Hellenischen Polizei Michalis Karamalakis, der Leiter der Wirtschaftsstaatsanwaltschaft Christos Barkadis, die Staatsanwältin Eleni Vlachou, der Regierungssprecher Giannis Oikonomou und der stellvertretende Leiter des EYP Vassilis Grizis. Die Enthüllungen auf der Liste sind nicht nur wegen der hochkarätigen Namen beunruhigend, sondern auch, weil Spähsoftware systematisch und in großem Stil missbraucht wird.

237. Im Jahr 2023 berichtete die ADAE, dass der EYP auch einen aktiven Minister, mehrere

[384] Sitzung des PEGA-Ausschusses, 20. April 2023.
[385] https://www.marieclaire.gr/art-lifestyle/artemis-seaford-i-chiroteri-morfi-katapiesis-ine-afti-pou-den-katalavenis-oti-ifistase/.
[386] *https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html#:~:text=Artemis%20Seaford%2C%20a%20dual%20U.S.,of%20illicit%20snooping%20in%20Europe*.
[387] Sitzung des PEGA-Ausschusses, 20. April 2023.

Offiziere, die sich mit Waffenfällen befassten, und einen ehemaligen nationalen Sicherheitsberater abgehört hat[388].

ABSCHLIEßENDE BEMERKUNGEN

238. Es gibt Muster, die darauf hindeuten, dass die griechische Regierung den Einsatz von Spähsoftware gegen Journalisten, Politiker und Geschäftsleute ermöglicht. Sie erlaubt zudem den Export von Spähsoftware in Länder mit einer katastrophalen Menschenrechtsbilanz und stellt ein Schulungszentrum für Agenten aus Drittländern bereit, die sich über Spähsoftware informieren möchten. Obwohl die Verwendung von Spähsoftware in Griechenland illegal ist, hat die Untersuchung der Herkunft der Spähsoftware-Angriffe erst im Sommer 2022 an Dynamik gewonnen. Politische Mehrheiten werden Berichten zufolge eher für die Förderung von Partikularinteressen als für das Allgemeininteresse genutzt, insbesondere durch die Ernennung von Verbündeten und Loyalisten in Schlüsselpositionen wie dem EYP, dem EAD (nationale Transparenzbehörde) und Krikel (ein auf elektronische Sicherheitssysteme spezialisiertes Unternehmen). Die höchste politische Führung im Land nutzt Spähsoftware als Werkzeug für politische Macht und Kontrolle, in einigen Fällen parallel oder nach rechtmäßiger Überwachung. Griechenland verfügt grundsätzlich über einen recht soliden Rechtsrahmen. Allerdings haben Gesetzesänderungen entscheidende Schutzmechanismen geschwächt und die politische Besetzung von Schlüsselpositionen behindert die Kontrolle und Rechenschaftspflicht. Die Mechanismen zur *ex ante*- und *ex post*-Kontrolle wurden bewusst geschwächt, und Transparenz und Rechenschaftspflicht werden umgangen. Kritische Journalisten oder Beamte, die sich gegen Korruption und Betrug engagieren, werden eingeschüchtert und behindert. Insgesamt ist das System der Schutzmechanismen und der Überwachung nicht ausreichend, um die Bürger vor Missbrauch durch staatliche Stellen und private Akteure zu schützen. Es muss noch mehr unternommen werden, um dieses Problem zu lösen. Darüber hinaus wird der Vorwand der „nationalen Sicherheit“ als Rechtfertigung für das Abhören von Einzelpersonen angeführt.

239. Die Ausspähung aus politischen Gründen ist in Griechenland nichts Neues, aber die neuen Spähsoftware-Technologien vereinfachen die illegale Überwachung um ein Vielfaches, insbesondere im Kontext stark geschwächter Schutzmaßnahmen. Im Gegensatz zu anderen Fällen, wie z. B. Polen, scheint der Missbrauch von Spähsoftware nicht Teil einer integralen autoritären Strategie zu sein, sondern eher ein Instrument, das ad hoc zum politischen und finanziellen Vorteil der Drahtzieher eingesetzt wird. Er untergräbt jedoch auch die Demokratie und die Rechtsstaatlichkeit und bietet reichlich Raum für Korruption, wo doch in diesen turbulenten Zeiten eine zuverlässige und verantwortungsvolle Führung gefragt ist.

I. D. Zypern

240. Der Ausschuss besuchte Zypern im November 2022 im Rahmen einer gemeinsamen Reise nach Griechenland und Zypern. Die Mitglieder trafen sich mit dem Minister für Energie, Handel und Industrie, anderen Regierungsbeamten und Mitgliedern des Repräsentantenhauses, die in den zuständigen Ausschüssen tagten, um den aktuellen

[388] Politico. *Brussels Playbook: Globalization’s sanatorium - Vestager rings alarm - S(uspended) & D(umped).*

Rechtsrahmen für Spähsoftware zu erörtern. Sie hörten auch Rechtsexperten, Vertreter von Nichtregierungsorganisationen und Journalisten an, die dem Ausschuss Unterlagen über Überwachung und Korruption übermittelten. Der Ausschuss betonte, dass bei den Registern der wirtschaftlichen Eigentümer mehr unternommen werden sollte. Diesen mangelt es an Transparenz, obwohl sie darauf ausgerichtet sind, genau solche Fragen zu beleuchten.

241. Im Gegensatz zu anderen Mitgliedstaaten gibt es nicht viele Informationen über die Verwendung von Spähsoftware durch Zypern. Es gibt keine offiziell bestätigten Fälle von Personen, die illegal mit Spähsoftware überwacht wurden. Allerdings wurde der Journalist Makarios Drousiotis angeblich von der zyprischen Regierung im Februar 2018 sowohl mit Abhörtechniken als auch mit Spähsoftware überwacht[389]. Auf dem Papier bietet das Land, indem auch die EU-Gesetze Anwendung finden, einen soliden Rechtsrahmen. In der Praxis jedoch ist Zypern ein attraktiver Standort für Unternehmen, die Überwachungstechnologien verkaufen. Die Regierung bestreitet dies jedoch und weist auf einen Rückgang der zugelassenen Spähsoftware-Unternehmen im Land hin. Die jüngsten Skandale haben dem Ruf des Landes jedoch geschadet. Eine Reihe neuer Gesetzesinitiativen zur Verschärfung des Rechtsrahmens für Ausfuhren und zur Verbesserung der Einhaltung der Vorschriften wird voraussichtlich 2023 abgeschlossen sein.

242. Im Zusammenhang mit Spähsoftware gibt es enge Verbindungen zwischen Zypern und Griechenland. Das Unternehmen Intellexa von Tal Dilian hat seinen Sitz in Griechenland, und seine Spähsoftware Predator wurde bei den griechischen Hacking-Skandalen eingesetzt. Beide Länder waren auch am illegalen Export der Predator-Spähsoftware an die sudanesischen Milizen der Rapid Support Forces (RSF) beteiligt[390]. Griechenland erteilte eine Ausfuhrgenehmigung, während das Material vom Flughafen Larnaca in den Sudan versandt wurde[391].

243. Neben der Ausfuhr von Spähsoftware in Länder außerhalb der EU erleichtert Zypern auch den Handel mit Subsystemen und Spähsoftwaretechnologie in die Mitgliedstaaten. Die Firma UTX Technologies – in Zypern eingetragen und vom israelischen Technologieriesen Verint übernommen – ist auf Rechnungen an deutsche, französische und polnische Unternehmen aufgetaucht, die Gi2-Technologie und Überwachungssysteme geliefert haben[392].

244. Auf dem Papier ist ein rechtlicher Rahmen gegeben, in dem der Schutz der privaten Kommunikation, die Verarbeitung personenbezogener Daten und das Recht des Einzelnen auf Information geregelt sind. In der Praxis gibt es jedoch keine eindeutigen Regeln für den Einsatz von Abhörgeräten und den Schutz der verfassungsmäßigen Rechte der Bürger, sobald die nationale Sicherheit geltend gemacht wird.

RECHTLICHER RAHMEN

[389] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/.
[390] LightHouse Reports. Flight of the Predator.
[391] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/.
[392] Philenews. Cyprus is a pioneer in software exports (documents).

245. Zypern scheint bei Überwachungstechnologien eng mit Israel zusammenzuarbeiten. Zypern konsultierte Israel und die USA zur Reform seines Rechtsrahmens und seines Systems zur Kontrolle der Ausfuhr von Gütern mit doppeltem Verwendungszweck. Zypern ist ein beliebter Standort für zahlreiche israelische Spähsoftware-Firmen.

246. Die Ausfuhr von Gütern mit doppeltem Verwendungszweck wird vom Ministerium für Energie, Handel und Industrie in der Abteilung für Ausfuhrgenehmigungen für strategische Güter geregelt[393]. In seiner Antwort auf den PEGA-Fragebogen, der allen Mitgliedstaaten zugesandt wurde, gab Zypern an, dass es alle Anträge auf Ausfuhrgenehmigungen für Güter mit doppeltem Verwendungszweck auf Einzelfallbasis und in voller Übereinstimmung mit den einschlägigen Sanktionsregelungen überwacht und bewertet. Bei diesen Regelungen handelt es sich um das Global Human Rights Sanctions Regime der Europäischen Union sowie die Dual-Use-Verordnung der EU, die sich an den Kriterien des einschlägigen Gemeinsamen Standpunkts des Rates (2008/944/GASP) orientiert[394]. Der PEGA-Ausschuss stellt fest, dass Zypern nicht am Wassenaar-Arrangement über Ausfuhrkontrollen für konventionelle Waffen sowie Güter und Technologien mit doppeltem Verwendungszweck beteiligt ist. Es wurde festgestellt, dass die Türkei die Teilnahme Zyperns an diesem Arrangement während der Reise des PEGA-Ausschusses blockierte. Die Regierung erklärt jedoch, dass sie sich an die gleichen Standards hält.

247. Das Ministerium für Energie, Handel und Industrie kann in Fragen der Erteilung von Ausfuhrlizenzen den sogenannten Beratenden Ausschuss konsultieren. Dieser Ausschuss besteht u. a. aus Vertretern des Verteidigungsministeriums, des Ministeriums für Justiz und öffentliche Ordnung, des Außenministeriums sowie der Zoll- und Verbrauchsteuerabteilung[395]. Nach Angaben der zyprischen Regierung wird dieser Ausschuss regelmäßig konsultiert, wenn Ausfuhranträge geprüft werden. In mehreren Fällen wurde die Ausfuhr von Gütern mit doppeltem Verwendungszweck in Drittländer abgelehnt, nachdem dieser Ausschuss eine ablehnende Stellungnahme abgegeben hatte[396]. Die Handelskammer macht in der Regel keine Angaben über die Zahl der genehmigten und abgelehnten Lizenzen für die Vermarktung von Software[397].

248. Während der Reise des PEGA-Ausschusses nach Zypern am 1. und 2. November 2022 trafen die Teilnehmer der Reise mit dem Ministerium für Energie, Handel und Industrie sowie dem stellvertretenden Minister für Forschung, Innovation und Digitalpolitik zusammen. Die Minister Natasa Pilides und Kyriacos Kokkinos erklärten, dass die Zahl der Unternehmen, die auf Zypern im Bereich Spyware tätig sind, stark zurückgegangen sei. 32 Firmen waren registriert, doch laut Minister waren zum Zeitpunkt des Besuchs nur acht bis zehn aktiv, von denen drei oder vier Spyware produzieren[398]. Sie räumten jedoch auch technische Herausforderungen bei der Überwachung und Steuerung von

[393] http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument.
[394] Antwort Zyperns auf den Fragebogen des Europäischen Parlaments.
[395] Lelaw, „Export Controls for dual-use products".
[396] Antwort Zyperns auf den Fragebogen des Europäischen Parlaments.
[397] Inside Story, „Who signs the exports of spyware from Greece and Cyprus?"
[398] Treffen mit Natasa Pilides, Ministerin für Energie, Handel und Industrie, und Kyriacos Kokkinos, stellvertretender Minister für Forschung, Innovation und Digitalpolitik, während der PEGA-Mission am 2. Februar 2022.

Unternehmen mit Sitz in Zypern ein, die einzelne Spyware-Komponenten unabhängig voneinander verkaufen.

249. In der Realität ist Zypern Berichten zufolge recht großzügig, wenn es um die Erteilung von Ausfuhrlizenzen für Spähsoftware geht[399]. Die Unternehmen wenden Techniken an, um die Vorschriften zu umgehen: Die physische Hardware des Produkts wird in ein Empfängerland geschickt, ohne dass die Software darauf hochgeladen wurde[400]. Im Anschluss wird die Aktivierungssoftware (auch als „Lizenzschlüssel“ bezeichnet) separat auf einem USB-Stick in das Zielland geschickt[401]. Eine andere Möglichkeit besteht darin, anzugeben, dass das Produkt nur zu Demonstrationszwecken ausgefahren wird – selbst wenn eine detaillierte Beschreibung des Produkts enthalten ist[402]. Darüber hinaus werden in den Formularen für Ausfuhrlizenzen unklare Beschreibungen der Spähsoftware angegeben, was angemessene Zollkontrollen behindert hat.

250. Mehrere zyprische Unternehmen haben Berichten zufolge Ausfuhrgenehmigungen für den Verkauf von Gütern mit doppeltem Verwendungszweck in Nicht-EU-Staaten erhalten. Diese Unternehmen sind UTX Technologies, Coralco Tech, Prelysis und Passitora[403].

251. UTX Technologies war am Verkauf von Spähsoftware an EU-Mitgliedstaaten sowie an Nicht-EU-Staaten beteiligt. Zwischen 2013 und 2014 wurde UTX auf Rechnungen an deutsche (Syborg Informationsysteme), französische (COFREXPORT) und polnische (Verint) Unternehmen für den Handel mit Überwachungssystemen und Gi2-Technologie erwähnt[404].

252. Die zyprische Handelsbehörde hat der Cognyte-Tochter UTX Technologies befristete Ausfuhrlizenzen für den Verkauf von Überwachungssoftware an Mexiko, die Vereinigten Arabischen Emirate, Nigeria, Israel, Peru, Kolumbien, Brasilien und Südkorea erteilt[405]. UTX Technologies hatte Berichten zufolge auch einen Vertrag mit Thailand über den Verkauf von Überwachungsteilsystemen im Wert von 3 Millionen USD. In der Beschreibung dieser Teilsysteme wurde auf eine Ausführung mit doppeltem Verwendungszweck mit Sprachanalysealgorithmus und Metadaten und Stimme verwiesen. Die Vereinbarung enthielt auch einen konkreten Verweis auf ein litauisches Unternehmen. Da die zyprischen Behörden die Ausfuhrgenehmigung nicht erteilen wollten, konnte das Ministerium für Energie, Handel und Industrie über die in Litauen eingetragene UAB Communication Technologies umgangen werden[406]. Dieses Unternehmen gehört dem russisch-israelischen Staatsangehörigen Anatoly Hurgin, der auch noch einen maltesischen Pass besitzt[407]. Außerdem hat UTX im Jahr 2019 einen Vertrag mit Bangladesch über ein Web Intelligence System für 2 Millionen USD und

---

[399] InsideStory, „Who signs the exports of spyware from Greece and Cyprus?“.
[400] InsideStory, „Who signs the exports of spyware from Greece and Cyprus?“.
[401] Philenews, „This is how interception patents are exported from Cyprus“.
[402] Philenews, „Export of monitoring software confirmed“.
[403] Philenews, „Cyprus is a pioneer in software exports (documents)“; Haaretz, „Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record“.
[404] Philenews, „Cyprus is a pioneer in software exports (documents)“.
[405] Philenews, „Cyprus is a pioneer in software exports (documents)“.
[406] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
[407] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.

im Jahr 2021 über ein zellulares Ortungssystem für 500 000 Dollar abgeschlossen[408].

253. Durch die zyprische Exportgeschichte wird auch ersichtlich, dass Coralco Tech – ursprünglich aus Singapur, aber auch in Israel und Nikosia eingetragen – nach einer Ausschreibung im Jahr 2018 Überwachungsausrüstung für 1,6 Millionen USD an das Militär von Bangladesch geliefert hat. Der Eigentümer von Coralco Tech ist der Israeli Eyal Almog[409].

254. Im Jahr 2019 kaufte der Inlandsgeheimdienst von Bangladesch (NSI) eine Software zum Abhören von WLAN von dem in Zypern registrierten Unternehmen Prelysis für insgesamt 3 Millionen USD. Kobi Naveh – der Gründer und Leiter von Prelysis – war bis 2014 für das israelische Unternehmen Verint tätig. Verint ist auch das Unternehmen, das das Zypern registrierte Unternehmen UTX Technologies übernommen hat[410].

255. Im Sommer 2021 kaufte Bangladesch zusätzlich ein Spionagefahrzeug von Tal Dilians Firma Passitora (ehemals WiSpear). Die auf den Britischen Jungferninseln eingetragene Schweizer Firma Toru Group Limited diente als Vermittler für die mit Dilians Passitora getroffenen Vereinbarungen[411].

256. Am 4. Oktober 2022 wurde enthüllt, dass das niederländische Verteidigungsministerium im November 2019 einen Vertrag mit WiSpear unterzeichnen wollte, dem Unternehmen von Tal Dilian, der zuvor Cytrox erworben hatte, dem Hersteller der Spähsoftware Predator[412]. Medienberichten und Erklärungen des DISY-Vorsitzenden (Dimokratikós Sinagermós) zufolge sendete WiSpeareine E-Mail an die Regierungspartei DISY und das Ministerium für Energie, Handel und Industrie, in der sie um Unterstützung bei der Umsetzung der Vereinbarung mit dem niederländischen Verteidigungsministerium ersuchten[413]. Es ist unklar, ob dieser Vertrag unterzeichnet wurde und ob dem niederländischen Verteidigungsministerium eine Spähsoftware zur Verfügung gestellt wurde.

257. Diese Beispiele zeigen, dass die Überwachungsindustrie auf Zypern sehr aktiv ist und dieselben Akteure involviert sind, die auch in dem Spähsoftware-Skandal auftauchen, der von PEGA untersucht wird.

258. Viele israelische Unternehmen entscheiden sich für den Standort Zypern, um mit ihren Tätigkeiten am europäischen Markt zu beginnen[414]. Ferner haben verschiedene Quellen darüber berichtet, dass im Land circa 29 israelische Unternehmen ansässig sind[415]. Einige Quellen weisen auf einen engen Zusammenhang zwischen dem Handel mit Spähsoftware und den diplomatischen Beziehungen des Landes hin. Als Gegenleistung für die Erteilung von Lizenzen für israelische Unternehmen hat Zypern angeblich einige der Produkte erhalten, die diese Unternehmen entwickeln und exportieren, wie z. B. die

[408] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record“.
[409] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record“.
[410] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record“.
[411] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record“.
[412] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
[413] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
[414] Philenews. Revelations in Greece: Predator came from Cyprus.
[415] Makarios Drousiotis. Κράτος Μαφία. Kapitel 6. Veröffentlicht 2022.

Spähsoftware „Pegasus“ von NSO[416] sowie Spähsoftware-Material von WiSpear[417]. Zypern dient als Stützpunkt für den Handel mit israelischer Spähsoftware auf dem EU-Binnenmarkt sowie für die Ausfuhr von Spähsoftware in Nicht-EU-Staaten.

EX-ANTE-KONTROLLE

259. Das Gesetz über den Schutz der Vertraulichkeit privater Kommunikation 92(I)/1996 sieht vor, dass der Generalstaatsanwalt bei Gericht einen Antrag auf Erlass einer richterlichen Anordnung stellen kann, mit der das Abhören privater Kommunikation durch eine befugte Person genehmigt oder eine solche Genehmigung erweitert wird. Dieser Antrag des Generalstaatsanwalts an das Gericht setzt einen schriftlichen Antrag des Polizeichefs, des Kommandanten des zyprischen Nachrichtendienstes oder eines Untersuchungsrichters voraus. Die Bestimmungen über die Genehmigung können jedoch in Fällen außer Kraft gesetzt werden, in denen das Abhören privater Kommunikation im Sicherheitsinteresse Zyperns liegt oder zur Verhinderung, Ermittlung oder Verfolgung von Straftaten erforderlich ist.[418]

260. Nach der Antragstellung erteilt der Polizeichef – im Einvernehmen mit dem stellvertretenden Polizeichef und dem Kommandanten des zyprischen Nachrichtendienstes – den Bediensteten seiner Dienststelle oder den Bediensteten, die im Auftrag seiner Dienststelle tätig sind, eine schriftliche Genehmigung zum Abhören privater Kommunikation und/oder zum Zugang zu der Überwachungsausrüstung zum Zwecke der technischen Arbeit.[419]

261. Darüber hinaus sieht Artikel 4 Absatz 2 des Gesetzes 92(I)/1996 in der Fassung von 2020[420] vor, dass es niemandem gestattet ist, Vorrichtungen oder Maschinen einzuführen, herzustellen, zu bewerben, zu verkaufen oder anderweitig zu vertreiben, die in erster Linie entwickelt, produziert, angepasst oder hergestellt wurden, um das Abhören oder die Überwachung privater Kommunikation zu ermöglichen oder zu erleichtern. Ein Verstoß gegen diesen Artikel kann mit einer Geldstrafe von 50 000 EUR und/oder einer Freiheitsstrafe von bis zu fünf Jahren geahndet werden.[421] Diese Bestimmungen gelten nicht, wenn der Anbieter den Zentralen Nachrichtendienst (KYP), die Polizei und den Bevollmächtigten informiert und deren Genehmigung eingeholt hat. Diese Bestimmungen gelten nicht für die Überwachungssysteme, die vom Polizeichef und vom Kommandanten des KYP verwendet werden.[422]

EX-POST-KONTROLLE

262. In Zypern sieht das Gesetz über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und für den freien Datenverkehr aus dem Jahr 2018 vor, dass

[416] Makarios Drousiotis. Κράτος Μαφία. Kapitel 6. Veröffentlicht 2022.
[417] Inside Story, „Predator: the ‘spy’ who came from Cyprus“.
[418] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).
[419] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).
[420] CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020.
[421] Antwort Zyperns auf den Fragebogen des Europäischen Parlaments.
[422] Antwort Zyperns auf den Fragebogen des Europäischen Parlaments.

eine Person das Recht hat, über die Verarbeitung personenbezogener Daten informiert zu werden, wenn diese Daten verwendet werden oder die betreffende Person Gegenstand der Verarbeitung war.[423] Dieses Recht kann umgangen werden, wenn der Beauftragte für den Schutz personenbezogener Daten anders entscheidet, unter anderem aus Gründen der nationalen Sicherheit.[424]

263. Darüber hinaus wird mit dem 1996 verabschiedeten Gesetz zum Schutz der Vertraulichkeit privater Kommunikation festgelegt, dass der Generalstaatsanwalt im Falle der Überwachung privater Kommunikation durch Strafverfolgungsbehörden verpflichtet ist, die betroffene Person zu informieren. Die Person muss innerhalb einer Frist von höchstens 90 Tagen ab dem Datum der richterlichen Anordnung[425] oder innerhalb einer Frist von höchstens 30 Tagen nach Vollstreckung dieser richterlichen Anordnung informiert werden. Der Generalstaatsanwalt muss der betroffenen Person einen Bericht zukommen lassen, in dem der Erlass der richterlichen Anordnung, das Datum des Erlasses und die Tatsache, dass innerhalb dieses Zeitraums eine Überwachung oder ein Zugriff auf die private Kommunikation stattgefunden hat, aufgeführt sind. Diese Verpflichtung kann vorübergehend ausgesetzt werden, wenn der Generalstaatsanwalt entscheidet, dass die Zurückhaltung dieser Informationen unter anderem im Interesse der Sicherheit Zyperns liegt.[426] Das Gericht kann auch anordnen, dass die Informationen im Hinblick auf die Sicherheitsinteressen Zyperns nicht offengelegt werden.[427]

264. Die Verletzung des Schutzes der privaten Kommunikation stellt de jure eine Straftat dar. De facto wird die Illegalität einer solchen Handlung häufig durch die Berufung auf die nationale Sicherheit verdeckt.[428] Es gibt kein Gesetz, das regelt, unter welche Umständen die Polizei oder andere Nachrichtendienste Abhörgeräte einsetzen können, wer Verfahren für Abhörungen regelt oder wie der Schutz der verfassungsmäßigen Rechte der Bürger gewährleistet wird. Die einschlägigen Verordnungen und Protokolle stehen derzeit noch vor der Diskussion und Genehmigung im Repräsentantenhaus. Vorerst wird diese Aktivität ungeprüft fortgesetzt.[429]

RECHTSBEHELF

265. Die Rechtmäßigkeit der Maßnahmen des zyprischen Nachrichtendienstes wird von einem dreigliedrigen Ausschuss gemäß dem zyprischen Nachrichtendienstgesetz, dem Cyprus Intelligence Service Law 74(I)/2016, bewertet. Der dreigliedrige Ausschuss

---

[423] Gesetz 125(I) von 2018. https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf.

[424] Agentur der Europäischen Union für Grundrechte, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update.

[425] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).

[426] Agentur der Europäischen Union für Grundrechte, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update.

[427] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).

[428] Makarios Drousiotis, „Κράτος Μαφία“, Kapitel 6, 2022.

[429] Philenews. ‘Legal but uncontrolled interceptions’.

wird vom Ministerrat auf Empfehlung des Präsidenten der Republik ernannt.[430]

266. Das Gesetz 92(I)/1996 wurde im Jahr 2020 geändert und der Rahmen für die Aufsicht in der Republik gestärkt, insbesondere die Bestimmungen über den dreigliedrigen Ausschuss. Im Rahmen seines Mandats kann der Ausschuss *von Amts wegen* zu den Einrichtungen, der technischen Ausrüstung und dem archivierten Material des KYP Untersuchungen einleiten und Nachforschungen anstellen. Wie in Artikel 17A(1) des Gesetzes 92(I)/1996, geändert durch das Gesetz 13(I)/2020, vorgesehen, kann der Ausschuss auch Untersuchungen der Einrichtungen, der technischen Ausrüstung und des archivierten Materials der Polizei einleiten. Im Anschluss an diese Untersuchungen kann der Ausschuss die Angelegenheit für weitere Maßnahmen an den Generalstaatsanwalt, den Beauftragten für den Schutz personenbezogener Daten oder den Beauftragten für elektronische Kommunikation und Postregulierung übergeben. Der Ausschuss legt dem Präsidenten der Republik außerdem einen Jahresbericht vor, in dem er seine Tätigkeiten beschreibt, Bemerkungen und Empfehlungen formuliert und Versäumnisse aufzeigt.[431]

267. Der zypriotische Staatspräsident hat ein erhebliches Mitspracherecht bei der Zusammensetzung des Ausschusses, dem die Befugnis zuteil wird, kritische Untersuchungen zu den Handlungen des KYP einzuleiten. Darüber hinaus werden die Jahresberichte mit den Ergebnissen des Ausschusses in einem ersten Schritt zunächst an den Präsidenten übermittelt.[432] Zum Zeitpunkt der Erstellung dieses Berichts liegen keine Informationen über die genaue Zusammensetzung des Ausschusses, seine Arbeit oder die von ihm ausgeübte Kontrolle vor.[433]

SCHLÜSSELFIGUREN IN DER SPÄHSOFTWARE-BRANCHE

268. Tal Dilian hat bei vielen der Entwicklungen in Zypern und Griechenland eine Schlüsselrolle gespielt. 2017 erhielt er die maltesische Staatsbürgerschaft.[434] Tal Dilian hatte 25 Jahre lang verschiedene Führungspositionen in den israelischen Verteidigungskräften inne, bevor er 2002 aus dem Militär ausschied.[435] Er begann seine Karriere als „Geheimdienstexperte, Community Builder und Serial Entrepreneur“ in Zypern und gründete dann die Aveledo Ltd, die später in die Ws WiSpear Systems Ltd. umbenannt wurde, sowie zu einem späteren Zeitpunkt auch die Passitora Ltd.[436]

269. In Zypern stand Dilian in enger Verbindung zu Abraham Sahak Avni. Avni war früher bei den Spezialeinheiten der israelischen Polizei als Sonderermittler tätig.[437] Im November 2015 konnte er dank einer Investition in Immobilien im Wert von

[430] Antwort Zyperns auf den Fragebogen des Europäischen Parlaments.
[431] Antwort Zyperns auf den Fragebogen des Europäischen Parlaments; CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020.
[432] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[433] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[434] Regierung Maltas. Persons Naturalised Registered Gaz 21.12 („Registrierte eingebürgerte Personen Gaz 21.12“) https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf.
[435] https://taldilian.com/about/.
[436] Opencorporates, Passitora ltd.
[437] ShahakAvni. About Shahak Avni.

2,9 Millionen EUR die zypriotische Staatsbürgerschaft und einen „goldenen Pass“ erwerben.[438] Avni gründete die zypriotische NCIS Intelligence Services ltd[439], ein Unternehmen, das Berichten zufolge mit den mächtigsten Technologie-Unternehmen der Welt zusammenarbeitet.[440] NCIS Intelligence and Security Services lieferte zwischen 2014 und 2015 Sicherheitssoftware an das Polizeipräsidium und waren zwischen 2015 und 2016 für die Schulung von Mitarbeitern des Amtes für Kriminalitätsanalyse und Statistik zuständig.[441] Zu den Kunden des Unternehmens zählt auch die Regierungspartei Dimokratikós Sinagermós (DISY). Berichten zufolge war Avni für die Installation von Sicherheitsanlagen in den Büros der Partei zuständig.[442] Neben der Sicherheitsausrüstung von Avni wurden die Materialien von Dilian auch an die zypriotische Drogenbekämpfungsbehörde und die zypriotische Polizei verkauft.[443]

270. Zu einem bestimmten Zeitpunkt stellte die Abteilung für Verbrechensermittlung des Polizeipräsidiums Verstöße gegen die Vertraulichkeit privater Kommunikation im Zusammenhang mit Avnis Unternehmen fest. Die Polizei beschloss, den Fall nicht weiter zu verfolgen.[444]

271. Zwischen Dilian und Avni bestehen zahlreiche Verbindungen. Dilians Unternehmen WiSpear teilte sich in Larnaca ein Gebäude und einige Beschäftigte mit Avni.[445] 2018 gründeten die beiden Männer das Unternehmen Poltrex, das später in Alchemycorp Ltd. umbenannt wurde. Seinen Sitz im Novel Tower teilte Poltrex mit Avni[446], und das Unternehmen gehört auch dem Firmenverbund Intellexa Alliance an. Berichten zufolge war mit Avnis Beziehungen zur DISY-Partei der Boden für die Erprobung von Dilians Produkten bereitet.[447]

DILIANS SPÄHSOFTWARE IM TRANSPORTER

272. Nach dem Verkauf von Circles Technologies und der Gründung von WiSpear gründete Tal Dilian 2019 auch noch die Intellexa Alliance, die nach Angaben auf der Website ein EU-gestütztes und reguliertes Unternehmen ist, das dem Zweck dient, Technologien zur Stärkung von Nachrichtendiensten zu entwickeln und zu integrieren.[448] Mehrere Überwachungsanbieter sind unter die Marketingbezeichnung Intellexa Alliance versammelt, z. B. Cytrox, WiSpear(später umbenannt zu Passitora Ltd.), Nexa Technologies und Poltrex Ltd. Diese verschiedenen dem Firmenverbund von Dilian angehörenden Anbieter ermöglichen es Intellexa, seinen Kunden ein breites Sortiment von Überwachungssoftware und -dienstleistungen anzubieten.[449] Weitere Einzelheiten zur Firmenstruktur sind im Kapitel über die Spähsoftware-Branche zu finden.

---

[438] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[439] Philenews, „FILE: The state insulted Avni and Dilian.“
[440] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[441] Philenews, „FILE: The state insulted Avni and Dilian.“
[442] Tovima, „The unknown ‘bridge’ between Greece and Cyprus for the eavesdropping system.“
[443] Inside Story, „Predator: The ‘spy’ who came from Cyprus.“
[444] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[445] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[446] CyprusMail, „Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal“.
[447] Inside Story, „Predator: The ‘spy’ who came from Cyprus.“
[448] https://intellexa.com/.
[449] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.“

273. Am 5. August 2019 gab Dilian dem Forbes-Magazin ein Interview über seinen schwarzen WiSpear-Lieferwagen, in dem er die verschiedenen Spähsoftware-Fähigkeiten seiner Allianz vorstellte. Mit diesem 9 Millionen EUR teuren Lieferwagen konnten Geräte innerhalb einer Reichweite von 500 Metern gehackt werden.[450] Die durch das Forbes-Interview[451] ausgelöste öffentliche Aufmerksamkeit führte zu einer Untersuchung durch die zyprischen Behörden. Der Anwalt Elias Stefanou wurde als unabhängiger Ermittler für diese Untersuchung eingesetzt. Während dieser Untersuchung entdeckten die Behörden ein weiteres Unternehmen von Dilian, das am internationalen Flughafen Larnaca agierte.[452]

274. Am 16. Juni 2019 schloss Tal Dilian Berichten zufolge eine außervertragliche Vereinbarung mit Hermes Airports ab, um seine WiSpear-Geräte für den angeblichen Zweck der Verbesserung des Wi-Fi-Signals für Passagiere am internationalen Flughafen Larnaca zu nutzen, woraufhin drei Funk-LAN-Antennen installiert wurden.[453] Das israelische Unternehmen Go Networks, das nicht in Zypern registriert ist, war ebenfalls an den Verhandlungen beteiligt, die zu der Vereinbarung führten.[454] Der eigentliche Grund für die Vereinbarung war jedoch, die Abhörtechnologie von WiSpear zu testen. Die abgefangenen Passagierdaten wurden auf den Servern im Serverraum des Flughafens gespeichert. Dieser befindet sich in unmittelbarer Nähe des WiSpear-Büros in Larnaca, das auch von Avni genutzt wird.[455] Während des Zeitraums, in dem die Antennen in Betrieb waren, wurden Daten von 9 507 429 mobilen Geräten abgefangen.[456]

275. Nach Beschwerden gegen Dilian wurde berichtet, dass das israelische Unternehmen Go Networks mutmaßlich über verteilte Eigentumsstrukturen des Unternehmens in Irland mit Intellexa verbunden war. Ehemaligen hohen Vertretern von Israeli Go Networks wurden angeblich Spitzenpositionen bei Intellexa verschafft.[457] Ferner ergaben die polizeilichen Ermittlungen, dass WiSpear Ausfuhrgenehmigungen erteilt wurden für „Abhörausrüstung, konstruiert für die Extraktion von über die Luftschnittstelle übermittelten Sprachinformationen oder Daten“.[458][459] Die Unternehmen von Dilian haben nach Angaben der Handelskammer in den letzten zwei Jahren keine Ausfuhrgenehmigungen erhalten. Zum Zeitpunkt der Erstellung dieses Berichts bleibt unklar, wer diese Ausfuhrgenehmigungen erteilt hat.[460]

276. Die elektronischen Daten, die aus den beschlagnahmten Geräten für die Untersuchung extrahiert worden waren, wurden einer dreistufigen forensischen Untersuchung durch

[450] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.“
[451] Forbes, „A Multimillionaire Surveillance Dealer Steps Out Of The Shadows ... And His $9 Million Whatsapp Hacking Van.“
[452] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.“
[453] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.“
[454] Makarios Drousiotis, „Κράτος Μαφία“, Kapitel 6, 2022.
[455] Makarios Drousiotis, „Κράτος Μαφία“, Kapitel 6, 2022.
[456] Makarios Drousiotis, „Κράτος Μαφία“, Kapitel 6, 2022.
[457] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[458] Makarios Drousiotis. Κράτος Μαφία. Kapitel 6. Veröffentlicht 2022.
[459] Philenews. Export of tracking software from Cyprus.
[460] Inside Story, „Who signs the exports of spyware from Greece and Cyprus?“

die Polizei, einen akademischen Experten und Europol unterzogen.[461] Der Lieferwagen blieb in Polizeigewahrsam. Was mit der Überwachungsausrüstung geschehen ist, ist unklar. Mutmaßlich wurde sie an Dilian zurückgegeben, aber es scheint keine Bestätigung dafür zu geben.

277. Am 15. November 2021 wurde der Fall vor die Strafgerichte gebracht, wobei WS WiSpear Systems Ltd., Tal Dilian und zwei weitere WiSpear-Mitarbeiter angeklagt wurden. Anschließend hat Generalstaatsanwalt George Savvides das Verfahren gegen das Unternehmen WiSpear aufrechterhalten, das Strafverfahren gegen Dilian und die Angestellten wurde hingegen eingestellt.[462] Die Gründe für diese Entscheidung sind geheim. Der Generalstaatsanwalt könnte jedoch jederzeit beschließen, das Verfahren gegen die drei Personen wieder aufzunehmen.

278. WiSpear bekannte sich in 42 Anklagepunkten für schuldig und wurde am 22. Februar 2022 von dem Schwurgericht zu einer Geldstrafe 76 000 EUR verurteilt.[463] WiSpear gestand die Vorwürfe der illegalen Überwachung der privaten Kommunikation und der Verletzung des Datenschutzes.[464] Das Gericht veröffentlichte sein Endurteil, in dem es heißt: „Das Schwurgericht stellte fest, dass die dem Unternehmen vorgeworfenen Verstöße niemals vorsätzlich, durch Hacken oder Abhören begangen worden seien und dass niemals versucht oder beabsichtigt worden sei, Daten zu personalisieren. Das Gericht betonte, dass keiner Person Schaden zugefügt worden sei.“[465] Zusätzlich zu der vom Schwurgericht verhängten Geldstrafe erhielt WiSpear aufgrund von Verstößen gegen die DSGVO von der Beauftragten für den Schutz personenbezogener Daten, Irini Loizidou Nicolaidou, eine Geldbuße in Höhe von 925 000 EUR.[466] Obwohl bekräftigt wurde, dass der Vorfall mit dem schwarzen Lieferwagen Angelegenheiten von nationalem Interesse und im Zusammenhang mit kritischer Infrastruktur berührte, fielen die Sanktionen für die Täter äußerst milde aus. Dieser Vorfall könnte über die Verletzung der Privatsphäre der Fluggäste hinaus eine politische Bedeutung haben. Da Zypern in vielerlei Hinsicht an einem Knotenpunkt liegt, gibt es mehrere Nicht-EU-Länder, die möglicherweise ein Interesse daran haben könnten, Einblick in die Bewegungen von Reisenden auf dem Flughafen Larnaka zu erhalten: die Türkei, Israel, Russland und die USA zum Beispiel.

279. Die Oppositionspartei AKEL brachte ihre Empörung darüber zum Ausdruck, dass das Verfahren gegen Dilian und seine Beschäftigten eingestellt wurde, und prangerte die juristische Entscheidung als Vertuschungsmaßnahme des Generalstaatsanwalts an.[467] Schließlich hatte die zyprische Regierung angeblich Ausrüstung von Dilians Unternehmen gekauft, und einer der angeklagten Beschäftigten war mutmaßlich für NSO tätig und führte für den KYP Schulungen für die Pegasus-Spähsoftware durch.[468]

---

[461] Pressemitteilung des stellvertretenden Generalstaatsanwalts vom 10. August 2022 im Rahmen der PEGA-Mission in Zypern vom 2. November 2022.
[462] Financial Mirror, „Anger after ‚spy van‘ charges dropped.“
[463] Makarios Drousiotis, „Κράτος Μαφία“, Kapitel 6, 2022; Pressemitteilung des stellvertretenden Generalstaatsanwalts vom 10. August 2022 im Rahmen der PEGA-Mission in Zypern vom 2. November 2022.
[464] Financial Mirror, „Spy van company fined €76,000.“
[465] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.“
[466] CyprusMail. Israeli company that deployed ‘spy van’ fined €925,000 for data violations; Financial Mirror, „Anger after ‚spy van‘ charges dropped.“
[467] Financial Mirror. Anger after ‘spy van’ charges dropped.
[468] Makarios Drousiotis. Κράτος Μαφία. Kapitel 6. Veröffentlicht 2022.

Durch die Einstellung des Verfahrens war der fortwährende Schutz der Verbindungen zwischen Dilians Unternehmen und der zyprischen Regierung sichergestellt.[469] Der Generalstaatsanwalt hat sich geweigert, die Ergebnisse der Untersuchung herauszugeben, obwohl der PEGA-Ausschuss sie während seiner offiziellen Reise nach Zypern beantragt hat. Dieses Beispiel zeigt, dass es keine vollständigen rechtlichen Garantien für die Datenschutzrechte von Einzelpersonen durch Massenüberwachungsausrüstung gibt. Zwar sind auf dem Papier Rechtsmittel vorhanden, doch der Staat kann auf den Ausgang von Gerichtsverfahren Einfluss nehmen, sodass Einzelpersonen, die Opfer solcher Rechtsverstöße werden, im Grunde wehrlos sind. Die Untersuchung ergab außerdem, dass Zypern für auf Zypern ansässige Unternehmen zu einem Ort geworden ist, an dem sie selbst mit Überwachungsausrüstung experimentieren können.

UMZUG NACH GRIECHENLAND

280. Nach dem Vorfall mit dem Transporter und dem Gerichtsverfahren verlagerte Herr Dilian die Geschäftstätigkeit von Intellexa nach Griechenland, obwohl er Zypern nie verlassen hat. Angeblich plant er seine Rückkehr nach Tel Aviv.[470] Indirekte Verbindungen zwischen einigen in Zypern und Griechenland gemeldeten natürlichen und juristischen Personen machen offenbar, wie die Verlegung von Dilians Unternehmen nach Athen abgelaufen ist.[471] Im Folgenden werden einige der Namen genannt, die zu den Verbindungen zwischen Zypern und Griechenland gehören, wobei die zentrale Rolle von Intellexa SA in Griechenland im Kapitel über Griechenland näher erläutert wird.

281. Die gerichtlichen Ermittlungen führten dazu, dass die Tätigkeiten von Herrn Avni und Herrn Dilian bei Poltrex auf Yaron Levgoren übertragen wurden. Herr Levgoren hat seinen ständigen Wohnsitz in Kanada. Er wurde Aktionär, Direktor und Sekretär von Poltrex. Levgoren ist auch mit Intellexa in Griechenland verbunden.[472] Laut seinem Linkedin-Profil vertritt er derzeit das in Griechenland ansässige Intellexa-Unternehmen Apollo Technologies.

ANBIETER VON SPÄHSOFTWARE UND ZYPERN

282. Neben Intellexa Alliance war angeblich auch die NSO Group in Zypern ansässig. 2010 gründete Tal Dilian zusammen mit Boaz Goldman und Eric Banoun das Unternehmen Circles Technologies, dessen Spezialität der Verkauf von Systemen war, die die SS7-Schwachstelle ausnutzen.[473] Sechs Jahre später wurde Circles Technologies für knapp 130 Mio. USD an Francisco Partners verkauft, wovon Herr Dilian 21,5 Mio. USD erhielt. Diese Private-Equity-Gesellschaft mit Sitz in Kalifornien erwarb auf ähnliche Weise 90 % der NSO Group, wodurch Circles Technologies und NSO Group unter dem Namen L.E.G.D Company Ltd. zusammengeführt wurden; dieses Unternehmen wurde

[469] Makarios Drousiotis. Κράτος Μαφία. Kapitel 6. Veröffentlicht 2022.
[470] Intelligence Online, „Israeli cyber tsar Tal Dilian plans Tel Aviv return.“
[471] *Haaretz*, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.“
[472] Philenews, „How the spyware scandal in Greece is related to Cyprus.“
[473] Amnesty International, Operating from the Shadows.

am 29. März 2016 in Q Cyber Technologies Ltd. umbenannt.[474]

283. Laut der Antwort der zyprischen Regierung an den PEGA-Ausschuss gibt es in der Abteilung für Handelsregister und geistiges Eigentum keine eingetragene juristische Person der NSO Group. Die NSO Group hält keine Anteile an einer in Zypern registrierten juristischen Person. Allerdings haben einzelne Vorstandsmitglieder der NSO Group sechs Unternehmen entweder gegründet oder gekauft. Außerdem wurde die Pegasus-Spähsoftware offenbar weder in Zypern entwickelt noch offiziell aus Zypern exportiert.[475]

284. Die Expansion unter Francisco Partners zwischen 2014 und 2019 erstreckte sich auf sechs zyprische Unternehmen. Francisco Partners wurde durch die in Zypern eingetragene ITOA Holdings Ltd. ergänzt, die Muttergesellschaft von CS-Circles Solutions Ltd., Global Hubcom Ltd. und MS Magnet Solutions. Ms Magnet Solutions ist Eigentümerin von Mi Compass Ltd. Des Weiteren ist CS-Circles Solutions Ltd. Eigentümerin von CI-Compass Ltd. Zusätzlich zu den zyprischen Unternehmen besitzt CS-Circles Solutions Ltd. auch bulgarische Unternehmen. Die NSO Group hat erklärt, dass „die bulgarischen Unternehmen auf Vertragsbasis Forschungs- und Entwicklungsdienstleistungen für ihre jeweiligen zyprischen Tochtergesellschaften erbringen würden und die Netzwerkprodukte für den staatlichen Gebrauch exportierten“.[476]

285. Die zyprische Regierung bestreitet den Export und die Entwicklung von Pegasus. Am 21. Juni 2022 erklärte der NSO-Bedienstete Chaim Gelfad jedoch, dass die Unternehmen der NSO Group in Zypern und Bulgarien an Software zur Bereitstellung von Nachrichtendiensten beteiligt seien.[477] Laut einem Dokument, das von der Oppositionspartei AKEL dem Europäischen Parlament vorgelegt wurde, hat die NSO Group die Pegasus-Spähsoftware mutmaßlich über eine ihrer Tochterunternehmen in Zypern an ein Unternehmen in den Vereinigten Arabischen Emiraten exportiert. Eines der Tochterunternehmen hat dem fraglichen Unternehmen 7 Mio. USD für Dienstleistungen in Rechnung gestellt.[478] Diese Angaben können jedoch nicht bestätigt werden.

286. Berichten zufolge besaß die NSO Group auch in Zypern ein aktives Unternehmen, das angeblich ein Kundenservicecenter unterhielt. Im Jahr 2017 fand im Four Seasons Hotel in Limassol ein Treffen zwischen NSO-Bediensteten und saudi-arabischen Kunden zur Vorführung der neuesten Funktionen der Version 3 der Pegasus-Spähsoftware statt. Diese Version enthielt die neuartige Zero-Click-Funktion, die es ermöglichte, ein Gerät zu infizieren, ohne dass ein Link angeklickt werden musste, beispielsweise auf dem Wege eines verpassten WhatsApp-Anrufs. Die saudi-arabischen Kunden kauften die Technologie umgehend für 55 Mio. USD.[479][480] In diesem Zusammenhang muss erwähnt werden, dass das saudische Regime ein Jahr später, am 2. Oktober 2018, Jamal

[474] Amnesty International, Operating from the Shadows.
[475] Antwort Zyperns auf den Fragebogen des Europäischen Parlaments.
[476] Amnesty International, Operating from the Shadows.
[477] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[478] Akel-Bericht, PEGA-Mission nach Zypern.
[479] Makarios Drousiotis, Κράτος Μαφία, Kapitel 6, veröffentlicht 2022.
[480] Haaretz, „Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals.“

Khashoggi im saudi-arabischen Konsulat in der Türkei tötete, nachdem ihm nahestehende Personen mit der Pegasus-Software überwacht worden waren. Dies wird von NSO bestritten.

287. Nach Angaben von CitizenLab waren im Jahr 2020 25 staatliche Akteure Kunden von Circles Technologies. Zu diesen staatlichen Akteuren gehörten Belgien, Dänemark, Estland und Serbien.[481] Im Jahr 2020 schloss die NSO Group ihre Circles-Niederlassung in Zypern. Zum Zeitpunkt der Erstellung dieses Berichts ist unklar, welche Circles-Unternehmen noch operativ tätig sind.[482]

288. Die israelische Firma QuaDream ist ein weiteres Unternehmen, das Berichten zufolge mit dem Export seines Spähsoftware-Produkts „Reign" aus Zypern verbunden ist. Im April 2023 berichteten Medien, QuaDream habe seine israelische Niederlassung geschlossen.[483] Über InReach, ein seit 2017 in Zypern eingetragenes Unternehmen, wurden QuaDream-Produkte indirekt an Kunden verkauft und damit israelische Ausfuhrkontrollen umgangen. Die beiden Unternehmen befinden sich in einem laufenden Rechtsstreit.[484]

289. Der derzeitige Direktor und Sekretär von InReach ist A.I.L. Nominee Services Ltd. Dieses Unternehmen wurde bereits 2010 in Zypern eingetragen und sein Gründungsaktionär war der derzeitige stellvertretende Generalstaatsanwalt Savvas Angelides.[485] Herr Angelides verkaufte seine Anteile an A.I.L. Nominee Services am 16. Februar 2018 an Christos Ioannides, also wenige Wochen bevor dieser Verteidigungsminister wurde.[486] A.I.L. Nominee Services bleibt jedoch Direktor und Sekretär von InReach[487] und damit im Geschäft mit einem Unternehmen, das QuaDream-Produkte in Drittländer exportiert.

290. 2011 gründete Abraham Sahak Avni zusammen mit Michael Angelides, dem Bruder des ehemaligen Ministers und stellvertretenden Generalstaatsanwalts Savvas Angelides, ein Unternehmen. Dieses Unternehmen namens S9S wurde am 10. November 2011[488] mit Unterstützung der ehemaligen Anwaltskanzlei von Savvas Angelides beim Handelsregister eingetragen.[489] Darüber hinaus wurde A.I.L. Nominee Services Ltd als Sekretär von S9S identifiziert. Während dieser Zeit war Savvas Angelides noch der Hauptaktionär von A.I.L. Nominee Services.[490] Die Partnerschaft zwischen Michael Angelides und Herrn Avni wurde jedoch 2012 aufgelöst. Savvas Angelides wurde 2020 stellvertretender Generalstaatsanwalt und verantwortlich für die Untersuchung von

---

[481] CitizenLab. Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles.
[482] Amnesty International, Operating from the Shadows.
[483] https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadream-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000.
[484] Amnesty International, Operating from the Shadows.
[485] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://opencorporates.com/companies/cy/HE373827.
[486] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.
[487] https://opencorporates.com/companies/cy/HE373827.
[488] Politis, 'Interceptions' file: Classified Police Report (2016) shows he knew everything about Avni.
[489] Pressemitteilung, stellvertretender Generalstaatsanwalt vom 10. August 2022, wie auf der PEGA-Mission nach Zypern am 2. November 2022 erhalten.
[490] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://b2bhint.com/en/company/cy/s9s-ltd--%CE%97%CE%95%20296578; https://i-cyprus.com/company/433750.

Herrn Avni und Herrn Dilian im Fall des Überwachungstransporters.[491] In einer Pressemitteilung vom 10. August 2022 erklärte der stellvertretende Generalstaatsanwalt, dass weder er noch seine Verwandten eine Verbindung zu Tal Dilian hätten. In Bezug auf die Partnerschaft zwischen Michael Angelides und Herrn Avni erwähnte er, dass „die berufliche Zusammenarbeit von Anfang an nicht funktioniert hat, zusammen mit der Tatsache, dass die von meiner ehemaligen Kanzlei eingetragene Gesellschaft auf Anweisung meines Verwandten nie aktiviert wurde“ und daher nie „ein Hindernis für meine Beteiligung an der Entscheidung über den Fall des ‚schwarzen Transporters‘ darstellte“.[492] In der Pressemitteilung wird jedoch weder auf die im Juli 2010 aktivierte Gesellschaft A.I.L Nominee Services von Savvas Angelides[493] noch auf die Rolle des Unternehmens als Sekretär in der Partnerschaft zwischen seinem Verwandten und Herrn Avni in S9S Bezug genommen.

BLACK CUBE

291. Black Cube ist ein Unternehmen, das ehemalige Offiziere israelischer Nachrichtendienste wie Mossad engagiert. Das Unternehmen beschäftigt Einsatzkräfte mit gefälschten Identitäten. Laut *The New Yorker* verpflichtete der ehemalige CEO der NSO Group Shalev Hulio Black Cube, nachdem drei Rechtsanwälte– Mazen Masri, Alaa Mahajna und Christiana Markou – in Israel und Zypern gegen NSO und ein angeschlossenes Tochterunternehme klagten.[494] Im Jahr 2018 erhielten die drei Rechtsanwälte mehrere Nachrichten von sogenannten Bekannten bestimmter Firmen und Personen, die Treffen in London vorschlugen. Hulio erklärte, dass „Black Cube an der Klage in Zypern beteiligt gewesen sei“, da die Klage aus dem Nichts gekommen sei und er es verstehen möchte.[495] Black Cube war auch in Spionageskandale in Ungarn und Rumänien verwickelt.

KAUF UND EINSATZ VON SPÄHSOFTWARE DURCH ZYPERN

292. Neben der Schaffung eines günstigen Exportklimas für Spähsoftware-Unternehmen hat die zyprische Regierung in der Vergangenheit auch selbst Spähsoftware erworben. Außerdem hat Zypern angeblich auch selbst Überwachungssysteme verwendet. Zum Zeitpunkt der Erstellung dieses Berichts ist unklar, in welchen Fällen Zypern konventionelle Überwachungsmethoden oder Spähsoftware verwendet hat.

293. Nach den Wahlen von 2013 wurde Andreas Pentaras zum Leiter des zyprischen Nachrichtendienstes ernannt, während der Überwachungsexperte Andreas Mikellis für den Schutz der Kommunikation von Präsident Anastasiades zuständig war. Im selben Jahr besuchte Herr Mikellis Berichten zufolge die Überwachungsmesse ISS in Prag, wo er angeblich mit Hacking Team über den Kauf der sogenannten DaVinci-Software verhandelte[496]. Mit der DaVinci-Software war es möglich, Anwendungen eines

---

[491] Bericht von Fanis Makridis, PEGA-Mission in Zypern am 1. November 2022.
[492] Pressemitteilung, stellvertretender Generalstaatsanwalt vom 10. August 2022, wie auf der PEGA-Mission nach Zypern am 2. November 2022 erhalten.
[493] https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=271194&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1.
[494] The New Yorker, „How Democracies Spy on their Citizens.“
[495] The New Yorker, „How Democracies Spy on their Citizens.“
[496] Makarios Drousiotis, Κράτος Μαφία, Chapter 6, published in 2022.

Mobiltelefons zu infizieren, weshalb sie die offiziellen Anforderungen für die Aufhebung des Datenschutzes nicht erfüllte[497].

294. Die von WikiLeaks aufgedeckten Kontaktinformationen zwischen Herrn Mikellis und Hacking Team deuten darauf hin, dass Ausschreibungsverfahren umgangen wurden und das erworbene Überwachungssystem nicht ordnungsgemäß geprüft wurde. Berichten zufolge wurde die Software Anfang 2014 installiert und vier Mitarbeiter der KYP wurden geschult, darunter Herr Mikellis[498].

295. Als WikiLeaks den Kauf der Überwachungssoftware von Hacking Team aufdeckte, bestätigte der KYP, dass dieses System nur für nationale Zwecke verwendet worden sei[499]. Trotz des Kontakts zwischen Herrn Mikellis und Hacking Team[500] war es der Leiter des KYP Andreas Pentaras, der nach Bekanntwerden dieser Enthüllungen schließlich zurücktrat[501]. Andreas Pentaras wurde durch Kyriakos Kouros ersetzt.

296. Gemäß WikiLeaks war eine weitere Polizeibehörde laut Bericht ebenfalls am Kauf eines Kommunikationsüberwachungssystems von Hacking Team interessiert. Diese Abteilung versuchte, sich dieses System durch Sahak Avni zu sichern[5021a]. Es ist jedoch unklar, um welche Polizeidienststelle es sich hier handelt**.**

ZIEL MAKARIOS DROUSIOTIS

297. Ab Februar 2018 wurde der Investigativjournalist Makarios Drousiotis angeblich von der zyprischen Regierung mithilfe von Abhörtechniken und Spähsoftware überwacht[503]. In diesem Fall begann die Bespitzelung, als Herr Drousiotis Assistent des zyprischen EU-Kommissars für Humanitäre Hilfe und Krisenmanagement, Christos Stylianides, war und während seiner Recherchen zu den finanziellen Verbindungen zwischen Präsident Anastasiades und russischen Personen wie dem Oligarchen Dmitri Rybolowlew. Laut Herrn Drousiotis wurde der erste Überwachungsversuch durch die letztere Tätigkeit ausgelöst[504].

298. Im Zuge der Recherchen von Herrn Drousiotis zu den Verbindungen nach Russland wurden in den internationalen Medien Enthüllungen über die von Zypern aus tätige NSO Group bekannt, unter anderem bei der Vorstellung von Pegasus 3 in den Four Season Hotels. CitizenLab vermutete außerdem, dass Zypern eines der Länder ist, die die NSO-Technologien nutzen, um die Kommunikation der Computersysteme des britischen Außenministeriums abzuhören[505]. Zu diesem Zeitpunkt erinnerte sich Herr Drousiotis an mehrere Anzeichen dafür, dass Telefon mit der Pegasus-Spähsoftware infiltriert worden war, darunter ein verpasster WhatsApp-Anruf, eine rasche Entleerung

---

[497] Inside Story*,* Predator: The 'spy' who came from Cyprus.
[498] Makarios Drousiotis, Κράτος Μαφία, Chapter 6, published in 2022.
[499] Inside Story*,* Predator: The 'spy' who came from Cyprus.
[500] Makarios Drousiotis, Κράτος Μαφία, Chapter 6, published in 2022.
[501] CyprusMail*,* Intelligence chief resigns after spy tech revelations. https://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/.
[502] Inside Story, Predator: The 'spy' who came from Cyprus.
[503] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/
184 Makarios Drousiotis, Κράτος Μαφία, Kapitel 5, veröffentlicht 2022.
[504] Makarios Drousiotis, Κράτος Μαφία, Kapitel 5, veröffentlicht 2022.
[505] BBC, No 10 network targeted with spyware, says group.

des Akkus und eine häufige Überhitzung seines Geräts, ohne dass er es benutzt hatte[506]. In Anbetracht dieser Ereignisse glaubt Herr Drousiotis, dass die zyprische Regierung – insbesondere der zyprische Geheimdienst – hinter der Infizierung seines Telefons steckte.

299. Im Mai 2019 richtete Herr Drousiotis einen Brief an Präsident Anastasiades, in dem er seine Besorgnis hinsichtlich der Überwachung seines Telefons zum Ausdruck brachte, die möglichen Motive für diese Überwachung darlegte und den Präsidenten persönlich für alles, was ihm nach der Bespitzelung zustoßen könnte, verantwortlich machte. Präsident Anastasiades leitete das Schreiben an den derzeitigen Leiter des zyprischen Geheimdienstes Kyriakos Kouros weiter. Sowohl Herr Anastasiades als auch Herr Kouros haben den Vorwurf der angeblichen Überwachung mit der Pegasus-Software zurückgewiesen und bekräftigt, dass die NSO Group tatsächlich gar nicht in Zypern registriert sei[507].

300. In den folgenden Monaten gab es mehrere Einschüchterungsversuche, darunter das Verschwinden von Beweismaterial auf seinem Computer, die Abschaltung der Überwachungskameras im Haus von Herrn Drousiotis und die Verfolgung durch Fremde. Nachdem Herr Drousiotis seine Geschichte öffentlich gemacht hatte und eine Beschwerde bei der zyprischen Polizei einreichte, kontaktierte Herr Drousiotis Lambros Katsonis, Leiter der Abteilung für technische Unterstützung von Panda Security, einem zyprischen Unternehmen, das auf Antivirenausrüstung spezialisiert ist. Herr Drousiotis wusste jedoch nicht, dass die zyprische Regierung diese Antivirensoftware auch für ihre eigenen Geräte verwendet hat. Vor diesem Hintergrund scheint Herr Katsonis unter falschen Vorwand zu Herrn Drousiotis nach Hause geschickt worden zu sein, möglicherweise mit dem Ziel, die Geräte von Herrn Drousiotis weiter zu infiltrieren, wie vom KYP angeordnet[508].

301. Im Jahr 2019 wurde Herr Drousiotis auf verdächtige Einträge auf seinem Android-Telefon aufmerksam und kontaktierte den Google One Support, um sich bestätigen zu lassen, um welche Art von Einträgen es sich handelte. Google reagiert jedoch im Allgemeinen nicht auf Fragen zur Überwachung und verwies den betreffenden Kunden an die nationalen Strafverfolgungsbehörden1a.Obwohl Herr Drousiotis kein Vertrauen in die Polizei hatte, stimmte er zu, seine Geräte zur forensischen Untersuchung zu übergeben[509].

ABSCHLIEßENDE BEMERKUNGEN

302. Zypern verfügt über einen stabilen Rechtsrahmen für den Schutz personenbezogener Daten und der Privatsphäre, die Genehmigung von Überwachung und für Ausfuhren. In der Praxis lassen sich diese Regelungen jedoch offenbar leicht umgehen, und Politiker/Politikerinnen, Sicherheitskräfte und die Überwachungsbranche unterhalten enge Verbindungen zueinander. Augenscheinlich ist die laxe Anwendung der Regeln der Grund, der Zypern für den Handel mit Spähsoftware so attraktiv macht. Die bestehenden Vorschriften müssen besser umgesetzt werden. Zudem ist Zypern von

[506] Makarios Drousiotis, Κράτος Μαφία, Kapitel 5, veröffentlicht 2022.
[507] Makarios Drousiotis, Κράτος Μαφία, Kapitel 5, veröffentlicht 2022.
[508] Makarios Drousiotis. Κράτος Μαφία. Kapitel 5. Veröffentlicht 2022.
[509] Makarios Drousiotis. Κράτος Μαφία. Kapitel 5. Veröffentlicht 2022.

erheblichem strategischem Interesse für Russland, die Türkei und die USA. Mit Blick auf den Handel mit Spähsoftware erscheinen enge Beziehungen zu Israel des Weiteren von besonderem gegenseitigem Nutzen. In diplomatischen Beziehungen sind Ausfuhrgenehmigungen für Spähsoftware zu einer Währung geworden.

Beispiel Spanien

303. Auf Einladung des PEGA-Ausschusses wurden die spanischen Behörden zu einer Anhörung am 29. November 2022 gebeten, um den Einsatz von Spähsoftware in Spanien so weit wie möglich im Rahmen ihrer rechtlichen Verpflichtungen zu erläutern. Aufgrund dieser „rechtlichen Einschränkungen“ waren die Antworten vor dem Ausschusses begrenzt und ließen die meisten Fragen unbeantwortet.

304. Der PEGA-Ausschuss besuchte Madrid im März 2023. Die Delegation traf sich mit dem Staatssekretär für europäische Angelegenheiten und Personen, die laut CitizenLab mittels Spähsoftware ins Visier genommen wurden, nämlich dem Präsidenten der Regionalregierung Kataloniens, dem katalanischen Regionalminister für auswärtige Angelegenheiten und einem Ratsmitglied des Stadtrats von Barcelona. Sie trafen auch Mitglieder des Untersuchungsausschusses des katalanischen Parlaments zu Pegasus, einem Vertreter des Büros des Bürgerbeauftragten, NGOs, die im Bereich der Grundrechte arbeiten und Journalisten.

305. Die Enthüllungen vom Juli 2021 im Zuge der Pegasus-Recherchen brachten zahlreiche mutmaßliche Ziele in Spanien ans Licht. Allerdings scheint es, dass unterschiedliche Akteure aus unterschiedlichen Gründen an diesen Aktivitäten beteiligt waren. Im Mai 2022 wurde in einem in der Tageszeitung *The Guardian* veröffentlichten Bericht Marokko als potenzieller Urheber der Ausspähung von mehr als 200 spanischen Mobiltelefonen genannt. Die spanische Regierung bestätigte, dass der Ministerpräsident Pedro Sánchez, die Verteidigungsministerin Margarita Robles und der Innenminister Fernando Grande-Marlaska mit der Pegasus-Spähsoftware infiziert wurden, während der Landwirtschaftsminister Planas ins Visier genommen, aber nicht infiziert wurde[510]. Auch sei das Mobiltelefon der damaligen Außenministerin Archa González Laya ausgespäht worden – obwohl weder der Ursprung des Cyberangriffs noch die Tatsache, dass es sich bei dem verwendeten System um Pegasus handelte, nachgewiesen werden konnten. Die Ausspähung einer zweiten Gruppe von Einzelzielen wird als „CatalanGate“ bezeichnet[511]. Betroffen waren in diesem Fall katalanische Parlamentarier, Mitglieder des Europäischen Parlaments, Rechtsanwälte, Journalisten, Angehörige zivilgesellschaftlicher Organisationen, Akademiker und einige Familienangehörige und Beschäftigte, die mit diesen Opfern[512] in Verbindung stehen und die als „indirekte“ oder „verbundene“ Zielgruppe bezeichnet werden können Erste Berichte über den Überwachungsskandal „CatalanGate“ erschienen im Jahr 2020 nach einer gemeinsamen Untersuchung von *The Guardian* und *El País*[513], aber erst im

[510] Le Monde, https://www.lemonde.fr/en/international/article/2022/05/10/spain-fires-head-of-intelligence-services-over-pegasus-phone-hacking_5982990_4.html, 10. Mai 2022.
[511] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022.
[512] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022*, Seite 1.
[513] https://www.theguardian.com/world/2020/jul/16/two-catalan-politicians-to-take-legal-action-targeting-spyware

April 2022 schloss CitizenLab eine eingehende Untersuchung ab und das Ausmaß des Skandals wurde offenbart. Die Untersuchungen ergaben, dass mindestens 65 Personen zu Zielscheiben der Ausspähaktion wurden.[514] Es sei darauf hingewiesen, dass CitizenLab im Dezember 2022 eingeräumt hat, dass eine Infizierung aufgrund eines Fehlers bei der Zuweisung von Initialen falsch zugeordnet wurde[515], wobei die Gesamtzahl der katalanischen Zielpersonen unverändert blieb. Im Mai 2022 gaben die spanischen Behörden zu, 18 Personen mit gerichtlicher Genehmigung[516] überwacht zu haben, die gerichtlichen Genehmigungen für diese Fälle wurden jedoch nicht veröffentlicht. Die ehemalige Direktorin des spanischen Geheimdienstes (CNI) Paz Esteban erschien in einer Sitzung unter Ausschluss der Öffentlichkeit vor dem Ausschuss für Staatsgeheimnisse des Parlaments, um die Überwachung dieser 18 Personen zu rechtfertigen.

306. Die spanische Regierung hat bisher nur begrenzt Informationen über ihre Rolle bei diesen Angriffen gegeben und sich dabei auf die Notwendigkeit der Vertraulichkeit im Hinblick auf die nationale Sicherheit berufen. Auf der Grundlage einer Reihe von Indikatoren[517], von denen einige vom oben genannten Ausschuss für Staatsgeheimnisse bestätigt wurden, wird jedoch davon ausgegangen, dass die Überwachung der katalanischen Zielpersonen von den spanischen Behörden durchgeführt wurde.

307. Durch eine genaue Analyse der Überwachung zeigt sich ein eindeutiges Muster. Die meisten Abhörmaßnahmen im Rahmen von CatalanGate fallen mit zentralen politischen Ereignissen, Themen oder Personen zusammen und beziehen sich auf diese, wie etwa die Zulässigkeit der Gesetze des katalanischen Parlaments zur Abspaltung, Gerichtsverfahren gegen katalanische Separatisten, von Tsunami Democràtic organisierte öffentliche Kundgebungen und die Kommunikation mit außerhalb Spaniens lebenden katalanischen Separatisten[518]. Diese Überwachung umfasst beispielsweise die Kommunikation zwischen einem inhaftierten Separatisten und seinem Anwalt am Vorabend seines Prozesses, Kontakte zwischen Ehepartnern oder die Kommunikation im Zusammenhang mit dem Einzug in das Europäische Parlament. Hinsichtlich der übrigen 47 Nutzungsfälle von Spähsoftware konnte nicht ermittelt werden, inwieweit die Zielpersonen einen unmittelbaren Einfluss auf die nationale Sicherheit oder die Integrität des Staates gehabt hätten oder inwieweit sie eine unmittelbare Bedrohung für diese darstellten, und es wurden keine Informationen dazu vorgelegt[519]. Obwohl einige Zielpersonen bereits vor ihrer Überwachung strafrechtlich verfolgt wurden, ist gegen keine der 18 Personen ein Strafverfahren basierend auf der Überwachung mit

---

514 Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18. April 2022,* Seite 1.

515 Citizen Lab*, Correcting a case,* CatalanGate report https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/ 22. Dezember 2022.

516 El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. Mai 2022.

517 Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, Seiten 1 + 3.

518 Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022.

519 Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022.

Spähsoftware eingeleitet worden[520].

KAUF VON SPÄHSOFTWARE

308. Die spanischen Behörden haben bereits 2001 den Kauf von Instrumenten zur Überwachung der Telekommunikation und den Erwerb von SITEL (Systems for the Lawful Interception of Telecommunications) eingeräumt. Sie räumten weiterhin ein, dass Spähsoftware-Dienste von Hacking Team im Jahr 2010 vom Innenministerium, dem CNI und der spanischen Polizei im Rahmen der Implementierung des integrierten Systems zur Überwachung der Telekommunikation beauftragt wurden, das den Einsatzeinheiten der Strafverfolgungsbehörden (FCSE) die Mittel für die Überwachung und Aufzeichnung der elektronischen Kommunikation, die durch eine richterliche Anordnung genehmigt wurde, zur Verfügung gestellt werden[521]. Seit seiner Anschaffung wurde SITEL von den spanischen Behörden unter anderem bei der Drogenbekämpfung, bei der Suche nach den Mitgliedern der Dschihad-Zelle, die hinter den Anschlägen vom 11. März 2004 in Madrid steckte, und bei der Bekämpfung von Fällen politischer Korruption eingesetzt. Früheren Berichten von CitizenLab zufolge wird Spanien außerdem verdächtigt, Kunde von FinFisher zu sein.[522] Die spanische Tageszeitung *El Pais* berichtete 2020, dass Spanien mit der NSO Group Geschäfte geschlossen hat und dass der spanische Geheimdienst CNI Pegasus routinemäßig nutzt.[523] Angeblich kaufte die spanische Regierung die Spähsoftware in der ersten Hälfte der 2010er Jahre für einen geschätzten Betrag von 6 Mio. EUR[524][525]. Der Kauf von SITEL wurde vom früheren Vizepräsidenten de la Vega im Jahr 2009[526] bestätigt, während die Vergabe von Diensten an Hacking Team vom CNI in einer Bemerkung gegenüber der Tageszeitung *El Confidencial* im Jahr 2015 eingeräumt wurde[527]. Außerdem hat ein ehemaliger NSO-Mitarbeiter bestätigt, dass Spanien ein Kundenkonto bei dem Unternehmen[528] unterhält, obwohl die spanischen Behörden nicht geneigt war, dies zu bestätigen oder zu kommentieren.[529]

309. Nach Angaben der Threat Analysis Group (TAG) von Google steht die in Barcelona ansässige Spähsoftware-Firma Variston IT angeblich in Verbindung mit einem Framework, mit dem N-Day-Schwachstellen in Microsoft Defender, Chrome und

---

[520] Mission to Spain.
[521] Ministerio del Interior, Secretaría de Estado de Seguridad, Centro Tecnológico de Seguridad, Homeland Security Project, scetse.ses.mir.es/publico/cetse/en/proyectosEuropeos/fondoISF/marcoFinanciero-2021-2027/proyectosEuISF.
[522] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, Seite 5.
[523] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, Seite 5.
[524] Politico, https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/, 20. April 2022.
[525] El Pais, https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html, 20. April 2022.
[526] Newtral, https://www.newtral.es/sitel-programa-espia-guardia-civil-policia-espana/20220509/ 9. Mai 2022.
[527] El Confidencial, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/ 6. Juli 2015.
[528] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens 18. April 2022.
[529] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. April 2022.

Firefox ausgenutzt werden und Spähsoftware auf Zielgeräten installiert wird. Diese Schwachstellen wurden 2021 und Anfang 2022 behoben[530]. Laut seiner Website bietet Variston „maßgeschneiderte Informationssicherheitslösungen“ an[531].

RECHTLICHER RAHMEN

310. Nach Artikel 18 der spanischen Verfassung von 1978 ist das Recht auf Privatsphäre, das das Post- und Fernmeldegeheimnis einschließt, geschützt[532]. Die Verwendung von Spähsoftware wie Pegasus und Candiru wäre ohne Vorliegen einer gerichtlichen Anordnung ein Verstoß gegen Artikel 18, aber diese Möglichkeit ist nach spanischem Recht vorgesehen[533]. Die Verfassung sieht in Teil I Abschnitt 55 weitere Ausnahmen zu diesen Rechten vor, denn dort heißt es, dass einige Rechte vorbehaltlich der Beteiligung der Gerichte und ordnungsgemäßer parlamentarischer Kontrolle ausgesetzt werden können, wenn der Ausnahmezustand oder der Belagerungszustand gemäß den in der Verfassung vorgesehenen Bedingungen verhängt wurde oder wenn gegen Personen wegen Aktivitäten im Zusammenhang mit bewaffneten Gruppen oder terroristischen Organisationen ermittelt wird[534]. Artikel 55 sieht auch demokratische Garantien vor, um sicherzustellen, dass die „ungerechtfertigte oder missbräuchliche Ausübung“ dieser Befugnisse zu einer strafrechtlichen Haftung führt.

311. Für Tätigkeiten, durch die die Unverletzlichkeit der Wohnung und des Kommunikationsgeheimnisses beeinträchtigt werden können, ist nach Artikel 18 der spanischen Verfassung eine richterliche Genehmigung erforderlich. Artikel 8 der EMRK fordert, dass jeglicher Eingriff in die Ausübung dieses Rechts durch eine Behörde im Einklang mit dem Gesetz stehen und eine Maßnahme darstellen muss, die in einer demokratischen Gesellschaft für die nationale oder öffentliche Sicherheit, das wirtschaftliche Wohl des Landes, die Aufrechterhaltung der öffentlichen Ordnung und die Verhütung von Straftaten, den Schutz der Gesundheit oder der Moral sowie den Schutz der Rechte und Freiheiten anderer notwendig ist.

312. Weitere Einzelheiten zu den Einschränkungen des Rechts auf Privatsphäre nach Artikel 18 sind in der Strafprozessordnung festgelegt[535] [536]. Artikel 588 dieses Gesetzes beschränkt insbesondere den Einsatz von Ermittlungsmaßnahmen auf die Untersuchung von Tatsachen, die aufgrund ihrer besonderen Schwere die Einschränkung der Grundrechte rechtfertigen. Die im Folgenden genannten Fälle sind jedoch von dieser Bestimmung ausgenommen: a) das Organisationsgesetz 2/2002 vom 6. Mai zur

---

[530] Threat Analysis Group. *New details on commercial spyware vendor Variston; Techcrunch. Spyware vendor Variston exploited Chrome, Firefox and Windows zero-days, says Google.*

[531] https://variston.net/.

[532] Spanische Verfassung 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, Abschnitt 18.

[533] Spanische Verfassung 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, Abschnitt 18.

[534] Spanische Verfassung 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, Abschnitt 55.

[535] Strafprozessordnung 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf.

[536] Königliches Dekret vom 14. September 1882 zur Genehmigung des Strafprozessrechts, https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20220907.

Regelung der vorherigen gerichtlichen Kontrolle des spanischen Geheimdienstes; b) das Organisationsgesetz 4/1981 vom 1. Juni über den Alarm-, Ausnahme- und Belagerungszustand; und c) das Organisationsgesetz 2/1989 vom 13. April über das militärische Verfahren, das ergänzende Bestimmungen zum Strafprozessrecht enthält. In Artikel 588 ist vorgesehen, dass die Genehmigung zur Überwachung des Telefon- und Telekommunikationsverkehrs von einem Richter erteilt wird, wenn die Ermittlungen schwere Straftaten wie Terrorismus oder Straftaten, die mit Hilfe von EDV-Instrumenten oder anderen Informations- oder Kommunikationstechnologien oder -diensten begangen werden, betreffen. Darüber hinaus müssen die Einschränkungen von einer Justizbehörde genehmigt werden. Für die Genehmigungen gelten vier konkrete Grundsätze: Erstens: Spezifischer Bezug (die Überwachung bezieht sich auf eine bestimmte Straftat); zweitens: Angemessenheit (Abgrenzung der Dauer, des Ziels und des subjektiven Anwendungsbereichs); Drittens: Verhältnismäßigkeit (Stärke der vorhandenen Beweise, Schwere des Falles und angestrebtes Ergebnis) und schließlich der Ausnahmecharakter und die Erforderlichkeit (es stehen keine anderen Maßnahmen zur Verfügung und ohne sie werden die Ermittlungen beeinträchtigt)[537]. In Artikel 588 *septies* (a., b. und c.) sind die Bedingungen für die Fernabfrage von Computern ausdrücklich festgelegt. Der zuständige Richter kann gemäß Artikel 588 *septies* die Installation von Software genehmigen, mit der eine Fern- und Telematikuntersuchung ohne Kenntnis des Eigentümers oder Benutzers ermöglicht wird, sofern sie in Verbindung mit der Untersuchung bestimmter Straftaten steht. Zu diesem Zweck ist die Maßnahme auf eine strikte Dauer von einem Monat begrenzt, die um einen Zeitraum von einem Monat bis zu einer Höchstdauer von drei Monaten verlängert werden kann.

313. In Artikel 197 des Strafgesetzbuchs ist eine Freiheitsstrafe von zwölf Monaten bis zu vier Jahren und eine Geldstrafe von zwölf bis 24 Monaten für Personen, die u. a. elektronische Post und Telekommunikation ohne ordnungsgemäße Genehmigung beschlagnahmen oder abfangen, vorgesehen[538]. Darüber hinaus regelt Artikel 264 der Strafprozessordnung die strafbare Handlung des Entfernens oder des Löschens von Daten und gestattet den Zugriff auf die Daten, wenn die erforderliche Genehmigung von einer zuständigen Behörde erteilt wurde[539].

314. Die Anforderungen an die gerichtliche Überwachung sind: a) die Kriminalpolizei muss den Untersuchungsrichter über die Durchführung und die Ergebnisse der Maßnahme informieren; b) in der genehmigenden gerichtlichen Entscheidung legt der Richter die Häufigkeit und Form fest, in der die Kriminalpolizei ihn über die Durchführung der Maßnahme unterrichten muss; c) innerhalb der festgelegten Fristen muss die Kriminalpolizei dem Richter zwei verschiedene digitale Dateien zur Verfügung stellen, eine mit der Transkription der als interessant erachteten Passagen und die andere mit den vollständigen Aufzeichnungen; d) in den Aufzeichnungen müssen Ursprung und

[537] Strafprozessordnung 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf.
[538] Strafgesetzbuch 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, Artikel 197.
[539] Strafgesetzbuch, 2016 https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf, Artikel 264.

Bestimmungsort der einzelnen Mitteilung angegeben werden; e) die Kriminalpolizei muss durch ein fortschrittliches elektronisches Versiegelungs- oder Unterschriftensystem oder ein ausreichend zuverlässiges Warnsystem die Authentizität und Integrität der Informationen sicherstellen, die vom Zentralcomputer auf die digitalen Datenträger, auf denen die Mitteilungen aufgezeichnet worden sind, übertragen werden; und f) die Kriminalpolizei muss bei Beendigung der Maßnahme über die Ergebnisse der Maßnahme berichten.

315. Der spanische Nachrichtendienst besteht im Wesentlichen aus drei Stellen. Erstens der nationale Geheimdienst CNI, der seine Aufgaben durch die Erhebung von Informationen in Spanien und in Drittstaaten wahrnimmt und der der Aufsicht und Kontrolle der exekutiven, legislativen und judikativen Gewalt unterliegt und dem Verteidigungsministerium angegliedert ist[540]. Der Direktor des CNI wird vom Verteidigungsminister ernannt und dient dem Ministerpräsidenten als leitender Berater in Fragen der nachrichtendienstlichen Aufklärung und Spionageabwehr.[541] Die zweite Stelle ist das Amt für Verfassungsschutz, das Zentrum für den Kampf gegen Terrorismus und organisierte Kriminalität (CITCO). Die dritte Stelle ist der spanische Militärgeheimdienst (CIFAS). Auch CIFAS untersteht der direkten Aufsicht des Verteidigungsministeriums.[542][543] Das CNI wurde durch das Gesetz 11/2002 vom 6. Mai 2002 gegründet, durch das ihm die Befugnis übertragen wurde, „sicherheitsrelevante Ermittlungen“ durchzuführen[544]. Die Polizei und Strafverfolgungsbehörde des Landes, die Guardia Civil, haben einen militärischen Charakter sind und auch dem Verteidigungsministerium unterstellt[545].

316. Das Gesetz über die Wahrung von Staatsgeheimnissen, das auf das Jahr 1968 zurückgeht, umfasst in Spanien als geheim eingestufte Dokumente und gibt keine Zeitspanne vor, nach der die Geheimhaltung eines Staatsgeheimnis nicht mehr erforderlich ist[546]. Sofern die Regierung Dokumente nicht explizit freigibt, d. h. die ausdrückliche Anordnung der Freigabe eines Dokuments durch ein Ministerium oder eine andere amtliche Stelle vorliegt, bleiben diese Dokumente geheim. Dieses Gesetz wird derzeit von der spanischen Regierung geprüft und obwohl es keine Frist für seine Verabschiedung gibt, wurde am 1. August 2022 ein Vorentwurf für ein Gesetz über Verschlusssachen genehmigt. Es sieht vor, dass Verschlusssachen innerhalb eines Zeitraums von vier bis 50 Jahren veröffentlicht werden müssen, wobei dieser Zeitraum verlängert werden kann.

EX-ANTE-KONTROLLE

317. Die Aufgabe des CNI ist es, die spanische Regierung mit den Informationen und

---

[540] Nationales Nachrichtenzentrum (CNI), https://www.cni.es/en/.
[541] https://www.cni.es/en/intelligence.
[542] https://emad.defensa.gob.es/en/?__locale=en.
[543]Geneva Centre for Security Sector Governance report 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf Seite 40.
[544] Gesetz 11/2002 6. Mai, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html Artikel 5.5.
[545] https://www.guardiacivil.es/es/institucional/Conocenos/index.html.
[546] El Pais, https://english.elpais.com/spanish_news/2021-04-05/spanish-government-begins-reform-of-franco-era-official-secrets-law.html, 5. April 2021; Official Secrets Act of 1968.

Erkenntnissen zu versorgen, die notwendig sind, um Risiken und Bedrohungen, mit denen die Unabhängigkeit und Integrität des Staates, die nationalen Interessen und die Stabilität des Rechtsstaats und seiner Institutionen beeinträchtigt werden, zu verhindern und abzuwehren. Die Überwachungsaktionen in Spanien wurden großteils vom CNI durchgeführt. Das CNI wurde mit dem Gesetz 11/2002 vom 6. Mai gegründet, das dem CNI die Befugnis einräumt, sicherheitsrelevante Ermittlungen gegen Personen oder Einrichtungen durchzuführen[547]. Es gibt jedoch wenig Klarheit darüber, welche Mittel oder Beschränkungen für solche Tätigkeiten verwendet werden oder gelten,[548]da die Tätigkeiten des CNI, seine Organisation und seine interne Struktur, Mittel und Verfahren, Personal, Einrichtungen, Datenbanken und Rechenzentren, Informationsquellen sowie Informationen oder Daten, die zur Kenntnis der oben genannten Angelegenheiten führen können, Verschlusssachen mit entsprechender Geheimhaltungsstufe sind[549]. Zudem sieht das Gesetz 11/2002 die parlamentarische, exekutive und legislative Aufsicht des CNI vor[550]. Die parlamentarische Kontrolle wird vom Ausschuss für die Verwendung und Kontrolle der den geheimen Fonds zugewiesenen Mittel (dem sogenannten Ausschuss für Staatsgeheimnisse) des Spanischen Parlaments ausgeübt, der 1995 eingerichtet wurde[551]. Aufgrund der verzögerten Besetzung des Ausschusses während der 14. Wahlperiode des spanischen Parlaments (das im Dezember 2019 gewählt wurde) hat der Ausschuss für Staatsgeheimnisse seinen Jahresbericht über die Tätigkeiten des CNI nicht wie gesetzlich vorgeschrieben vorgelegt. Bis April 2023 wurde in dieser Legislaturperiode kein Jahresbericht vorgelegt. Der Delegierte Ausschuss für nachrichtendienstliche Angelegenheiten der Regierung koordiniert die nachrichtendienstlichen Tätigkeiten aller spanischen Geheim- und Informationsdienste[552]. Der Verteidigungsausschuss des spanischen Abgeordnetenhauses schließlich übt die legislative Aufsicht über den CNI aus.[553] In der jährlichen nachrichtendienstlichen Direktive werden die nachrichtendienstlichen Prioritäten des CNI festgelegt.

318. Die gerichtliche Kontrolle über die Maßnahmen der CNI ist im Organisationsgesetz 2/2002 vom 6. Mai[554] [555]festgelegt, durch das das Gesetz 11/2002 vom 7. Mai zur Regelung des CNI ergänzt wird. Insbesondere verlangt diese Verordnung, dass der CNI, wenn er eine Überwachung durchführen will, verpflichtet ist, die Genehmigung eines zuständigen Richters des Obersten Gerichtshofs gemäß dem Gerichtsverfassungsgesetz zu beantragen, die Durchführung von Maßnahmen zu genehmigen, die die

[547] Gesetz 11/2002 vom 6. Mai, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, Artikel 5.5.
[548] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. Mai 2022.
[549] Gesetz 11/2002 vom 6. Mai, Regelung des spanischen Geheimdienstes, Artikel 5.1.
[550] Gesetz 11/2002 6. Mai, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, Artikel 11.
[551] Gesetz 11/1995 vom 11. Mai, https://www.boe.es/eli/es/l/1995/05/11/11/con.
[552] Gesetz 11/2002 vom 6. Mai, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, Artikel 6.
[553] Gesetz 11/2002 6. Mai, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, Artikel 11.
[554] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. Mai 2022.
[555] Organisationsgesetz 2/2002 vom 6. Mai, https://www.global-regulation.com/translation/spain/1451142/law-2-2002%252c-6-may%252c-regulating-the-prior-judicial-control-of-the-national-intelligence-center.html.

Unverletzlichkeit der Wohnung und des Kommunikationsgeheimnisses beeinträchtigen[556], sofern diese Maßnahmen für die Erfüllung der Aufgaben der CNI erforderlich sind. Darüber hinaus sieht das Gesetz vor, dass Überwachungsmaßnahmen nicht länger als drei Monate dauern dürfen und dass eine Verlängerung dieser Frist ordnungsgemäß begründet sein muss. Diese Bestimmungen wurden jedoch zu einer Zeit in Kraft gesetzt, als die Überwachungstechnologie noch nicht so weit fortgeschritten war und Spähsoftware wie Pegasus und Candiru noch nicht existierten. Daher besteht die Gefahr, dass die rechtlichen Garantien veraltet sind und den Bürgerinnen und Bürgern keinen ausreichenden Schutz bieten. Daher kündigte die Exekutive an, den Rechtsrahmen des CNI zu reformieren, bisher wurden aber noch keine Vorschläge vorgelegt.

EX-POST-KONTROLLE

319. Mit den Gesetzen zur Einrichtung des CNI wurde auch der Verteidigungsausschuss des Abgeordnetenhauses eingerichtet, der für die Zuweisung geheimer Mittel an den CNI und die Erstellung eines Jahresberichts über den CNI verantwortlich ist. Die Beträge, die den geheimen Fonds zugewiesen werden, sind im spanischen Gesetz über den Gesamthaushalt für jedes Haushaltsjahr festgelegt[557]. Alle Gremien, die mit der Aufsicht des CNI betraut sind, wie der Verteidigungsausschuss, der Ausschuss für Staatsgeheimnisse oder der Bürgerbeauftragte, haben Zugang zu den Informationen, die erforderlich sind, um zu beurteilen, ob die Operationen rechtmäßig und korrekt durchgeführt wurden. Die Regierung bestimmt und genehmigt die geheimen Ziele des CNI jährlich durch die Geheimdienstrichtlinie[558][559]. Der Direktor des CNI hat die ausschließliche Zuständigkeit für die Entscheidung über den Zweck und die Bestimmung der zugewiesenen Mittel und muss dem Premierminister regelmäßig über deren Verwendung Bericht erstatten. Der Ausschuss für Staatsgeheimnisse wird über die nachrichtendienstlichen Ziele informiert und hat das Recht, einen Jahresbericht über die Tätigkeit der Nachrichtendienste vorzulegen[560]. Er hat auch Zugang zum jährlichen Bericht des Direktors des CNI über die Bewertung der Tätigkeiten, des Status und des Grads der Erfüllung der Ziele. Das spanische Recht sieht jedoch nicht vor, der Öffentlichkeit Zugang zu Dokumenten oder Informationen in Bezug auf die Arbeit der Nachrichtendienste zu gewähren. Eine solche Vorgabe fehlt insbesondere im rechtlichen Rahmen des Gesetzes über Transparenz[561]. Angesichts dieser Geheimhaltung kann nicht mit Sicherheit festgestellt werden, ob die spanische Regierung Verträge mit der NSO-Gruppe geschlossen hat oder ob sie Pegasus erworben und genutzt hat. Die betroffenen Personen kennen die Gründe, den Umfang und die

[556] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. Mai 2022.
[557] Gesetz 11/1995 vom 11. Mai, Regelung der Verwendung und Kontrolle der den geheimen Fonds zugewiesenen Mittel, Artikel 2, https://www.boe.es/eli/es/l/1995/05/11/11/con.
[558] Gesetz 11/2002 vom 6. Mai, Regelung des spanischen Geheimdienstes (CNI), Artikel 3.
[559] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 2.
[560] Gesetz 11/1995 vom 11. Mai, Regelung der Verwendung und Kontrolle der den geheimen Fonds zugewiesenen Mittel Artikel 7.4.
[561] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 2.

Folgen der Überwachung ihrer Kommunikation nicht[562].

320. Infolge der Enthüllung, dass der CNI Pegasus und Candiru eingesetzt hat, kündigte der spanische Bürgerbeauftragte eine Untersuchung von Amts wegen an[563]. Der spanische Bürgerbeauftragte hat in seiner offiziellen Erklärung vom 18. Mai 2022 eingeräumt, dass der Ministerrat dem Bürgerbeauftragten vollen Zugang zu Verschlusssachen gewährt hat, ohne von seinem Vorrecht gemäß Artikel 22 des Organisationsgesetzes 3/1981 über den Bürgerbeauftragten Gebrauch zu machen. Diese Untersuchung bezog sich jedoch nur auf die 18 Personen, von denen die spanischen Behörden bestätigt haben, dass sie mit gerichtlicher Genehmigung ins Visier genommen wurden[564][565]. Die Untersuchung kam zu dem Schluss, dass die Überwachung im gesetzlich zulässigen Rahmen durchgeführt worden seien, weil festgestellt wurde, dass sie von einem Gericht genehmigt worden seien und die Genehmigung mit der erforderlichen Rechtfertigung verbunden sei[566]. Der Bürgerbeauftragte ist jedoch nicht befugt, die Verhältnismäßigkeit zu beurteilen, da diese nur von einem Richter bestimmt werden kann[567]. Er kontaktiere oder befragte auch keine der Zielpersonen oder deren Anwälte. Der Bürgerbeauftragte empfahl eine Überprüfung der geltenden Rechtsvorschriften und erforderlichenfalls Reformen, um der Modernisierung der Überwachungssysteme Rechnung zu tragen[568]. Daraufhin kündigte die spanische Regierung im Mai 2022 eine Überprüfung des Gesetzes über die Wahrung von Staatsgeheimnissen aus dem Jahr 1968 und des Organisationsgesetzes 2/2002[569] [570]an, ein Zeitrahmen für die Ausführung dieser Überprüfung wurde jedoch nicht festgelegt.

321. Der Ausschuss für Staatsgeheimnisse ist verpflichtet, einen jährlichen Bericht zu den Tätigkeiten der Geheimdienste einzureichen. Als dieser am 5. Mai 2022 angesichts der Überwachungsaktivitäten des CNI zusammenkam, war dies aufgrund der Unterbrechung der parlamentarischen Tätigkeiten wegen COVID-19 die ersten Sitzung der Einrichtung seit mehr als drei Jahren. Die Leiterin des CNI, Paz Esteban, erschien vor dem Ausschuss und räumte die Überwachung von 18 Anführern der separatistischen Bewegung ein. Darüber hinaus legte sie dem Ausschuss die gerichtlichen Anordnungen für diese 18 Fälle vor[571][572]. Gemäß Art. 5.5 des Gesetzes 11/2002 wurde die Anhörung

---

[562] Amnesty International - 10 medidas que garanticen la no repeticion de violaciones des Derechose Humanos.
[563] https://www.reuters.com/article/us-spain-politics-catalonia-spying-idCAKCN2MG0A6, 24 April 2022.
[564] The Guardian, https://www.theguardian.com/world/2022/may/05/catalans-demand-answers-after-spanish-spy-chief-confirms-phone-hacking, 5. Mai 2022.
[565] https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/.
[566] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. Mai 2022.

[567] Informationen aus „Mission to Spain".
[568] https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/.
[569] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. Mai 2022.
[570] https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. Mai 2022.
[571] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. Mai 2022.
[572] El País, https://elpais.com/espana/2022-05-05/la-directora-del-cni-da-explicaciones-sobre-el-espionaje-de-pegasus-ante-el-escepticismo-de-los-partidos.html, 21. Mai 2022.

jedoch unter Ausschluss der Öffentlichkeit durchgeführt und die Anwesenden durften keine elektronischen Geräten bei sich führen[573]. Abgesehen von der Anzahl der Fälle wurden keine offiziellen Informationen zur Verfügung gestellt. Laut den bei der Anhörung anwesenden Sprechern ging es fast ausschließlich um die katalanischen Opfer und nicht um Pedro Sánchez oder Margarita Robles und die angeblichen drei Gigabyte an Daten, die durch die „Söldner-Spähsoftware“ von ihren Geräten entwendet wurden[574]. Robles betonte mehrfach, dass die 18 Katalaninnen und Katalanen berechtigterweise Zielpersonen waren.

322. Sánchez hat sich auch im spanischen Parlament zu diesem Thema geäußert, wo er erneut betonte, dass alles im Rahmen des Gesetzes geschehen sei und dass die nationale Sicherheit der Aufsicht des Parlaments und anderer Regierungsstellen unterliege[575]. Die Behauptung, dass der Einsatz von Pegasus durch den CNI völlig legal sei, wurde auch vom ehemaligen CEO der NSO Group, Shalev Hulio, vertreten, als er gegenüber dem *New Yorker* erklärte, dass der Einsatz von Pegasus durch Spanien legitim sei, da Spanien die Rechtsstaatlichkeit stark respektiere und eine Genehmigung des Obersten Gerichtshofs verlange[576].

323. Am 3. Mai 2022 stimmte der spanische Kongress gegen einen Vorschlag zur Einsetzung eines Untersuchungsausschusses zur Verwendung von Pegasus. Am 21. September 2022 richtete das katalanische Parlament einen Untersuchungsausschuss hinsichtlich der Überwachung von politischen Vertretern, Aktivisten, Journalisten und ihren Familien durch das Königreich Spanien mithilfe der Programme Pegasus und Candiru ein.

ÖFFENTLICHE KONTROLLE

324. Seit dem Bekanntwerden der Enthüllungen im April 2022 ans Licht kam, hat sich die Öffentlichkeit eingehend mit dem Einsatz von Spähsoftware gegen Mitglieder der spanischen Regierung und Befürworter der katalanischen Unabhängigkeit befasst. Die spanischen Medien und Medienunternehmen weltweit haben zusammen mit Organisationen der Zivilgesellschaft intensiv daran gearbeitet, das Überwachungssystem in Spanien zu untersuchen und sich für die Grundrechte der Opfer einzusetzen. Im Gegenzug haben manche spanische Politiker versucht, CitizenLab zu diskreditieren, indem sie behaupteten, ihre Methoden seien unseriös oder politisch motiviert.

RECHTSBEHELF

325. Die Staatsanwaltschaft[577] hat beim spanischen nationalen Gericht in Madrid, der

---

[573] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. Mai 2022.
[574] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. Mai 2022.
[575] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. Mai 2022.
[576] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. April 2022.
[577] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. Mai 2022.

Audienca Nacional, eine Klage hinsichtlich der Überwachung durch Überwachungs- und Spähsoftware von Premierminister Pedro Sánchez und Verteidigungsministerin Margarita Robles eingereicht. Die Zuständigkeit des spanischen nationalen Gerichts wird in Artikel 65.1 a (des spanischen Gerichtsverfassungsgesetzes 6/1985 festgelegt, da davon hochrangige nationale Stellen wie der Premierminister und die Verteidigungsministerin betroffen sind. Der Richter José Luis Calama, Leiter des zentralen Ermittlungsgerichts Nummer 4 ist für diesen laufenden Fall verantwortlich[578]. Am 13. Oktober 2022 reichte Richter Calama einen an Robles und Grande-Marlaska gerichteten Fragebogen ein, der – wie Rechtsquellen bestätigen – die Anfrage enthielt, wie die Infizierung mit Pegasus ermittelt wurden. Die Staatsanwaltschaft und das Büro des Staatsanwalts übermittelten ebenfalls Fragen an die Ministerinnen und Minister[579].

326. Personen, die direkt oder indirekt mit der katalanischen Unabhängigkeitsbewegung in Verbindung stehen, haben beim Untersuchungsgericht in Barcelona Klagen wegen Überwachung durch Spähsoftware eingereicht, und die Untersuchungen laufen noch, wenn auch langsam. Die erste Beschwerde wurde im Jahr 2020 von Roger Torrent, ehemaliger Präsident des katalanischen Parlaments und derzeitiger Regionalminister für Wirtschaft und Arbeit von Katalonien, und Ernest Maragall, ehemaliger Regionalminister für auswärtige Angelegenheiten, institutionelle Beziehungen und Transparenz von Katalonien und derzeitiger Präsident der Esquerra Republicana de Catalunya (ERC) im Stadtrat von Barcelona, eingereicht[580][581]. Der Fall wurde dem Untersuchungsgericht Nr. 32 in Barcelona zugewiesen, das den Fall vorläufig geschlossen hat. Andreu Van Den Eynde ist einer der Anwälte, die Torrent und Maragall in diesem Fall vertreten, und selbst ein Zielperson von Pegasus. Van Den Eynde hat die Gerichte immer wieder dahingehend kritisiert, dass sie die Verfahren verzögern und den Fall geradezu „lähmen“[582]. Òmnium Cultural und die Katalanische Nationalversammlung (ANC), sowie die Partei Candidatura d’Unitat Popular (Kandidatur der Volkseinheit, CUP) haben ebenfalls mehrere Strafanzeigen bei demselben Gericht in Barcelona eingereicht, ohne dass bisher eine Untersuchung eingeleitet wurde. Das Untersuchungsgericht Nr. 32 in Barcelona lehnte den Antrag auf gemeinsame Klagen ab, sodass sich nun verschiedene Gerichte und verschiedene Richter mit verschiedenen Klagen befassen. Die Klagen von Òmnium Cultural und der CUP wurden am April 2022 dem Untersuchungsgericht 21 zugewiesen und die Fälle der ANC wurden am 26. Juli 2022 dem Gericht 23 zugewiesen. Die Beschwerden wurden weder vollständig fortgeführt, noch wurde vereinbart, Untersuchungen einzuleiten, sodass keiner dieser Fälle untersucht wird. Die meisten Fälle wurden von den Richtern zurückgehalten, bis weitere Beweise gesammelt werden, da die Hauptbeweise – die angeblich infizierten Mobiltelefone – sich nicht im Besitz der

[578] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. Mai 2022.
[579] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. Mai 2022.
[580] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. Mai 2022.
[581] El Diario, https://www.eldiario.es/catalunya/juez-archiva-investigacion-espionaje-pegasus-torrent-maragall_1_9030414.html, 30. Mai 2020.
[582] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30. Mai 2022.

Kläger befanden[583]. Die Richter können beschließen, die Berichte von CitizenLab als Sachverständigenbeweis in dem Fall zu akzeptieren. Sollten die Richter dies jedoch nicht zulassen, wird es für die betroffenen Personen schwierig, ihre Klage vor Gericht durchzusetzen[584].

327. Da das spanische nationale Gericht in ganz Spanien für die schwersten Straftaten zuständig ist, könnte die Staatsanwaltschaft die Zusammenlegung aller Pegasus-Fälle beantragen[585]. Die Fälle der Zielpersonen der spanischen Regierung und von „CatalanGate“ würden alle vor dem spanischen nationalen Gericht in Madrid verhandelt werden. Die Anwälte der katalanischen Zielpersonen vertreten, dass es keinen Zusammenhang zwischen den Fällen gibt, solange nicht bewiesen ist, dass der Täter in allen Fällen der Überwachung derselbe ist[586].

328. Es gibt eine Reihe anderer anhängiger Rechtssachen im Zusammenhang mit den 65 katalanischen Zielpersonen. Eines dieser Verfahren wurde von Rechtsanwalt und Zielperson von Pegasus Gonzalo Boye im Namen von mindestens 19 Personen gegen NSO, seine drei Gründer, Niv Karmi, Shalev Hulio und Omri Lavie, Q Cyber Technologies, und OSY, eine Tochtergesellschaft mit Sitz in Luxemburg, angestrengt[587][588]. Der frühere Präsident von Katalonien, Quim Torra, und der ehemalige Vizepräsident des Katalanischen Parlaments, Josep Costa, haben eine Beschwerde beim Obersten Gerichtshof eingereicht, aber ein Jahr später steht die Entscheidung der Justiz darüber, ob der Fall vor dem Obersten Gerichtshof oder dem nationalen spanischen nationalen Gericht verhandelt werden soll, weiterhin aus. Ermittlungen haben zwischenzeitlich nicht stattgefunden. Auch in Frankreich, Belgien, der Schweiz, Deutschland und Luxemburg wurden rechtliche Schritte zur Überwachung katalanischer Separatisten im Exil eingeleitet[589].

DIE ZIELPERSONEN

329. Die gezielte Ausspähung von Anhängern der katalanischen Unabhängigkeitsbewegung und deren Familien und Mitarbeitern mit Spähsoftware begann Berichten zufolge bereits 2015, als der damalige Präsident der Katalanischen Nationalversammlung (ANC), Jordi Sánchez, kurz nach einer großen Demonstration in Barcelona gezielt ins Visier genommen wurde. Laut dem CitizenLab-Bericht von April 2022 wurden zwischen 2017 und 2020 mindestens 65 Personen mit Spähsoftware ins Visier genommen: 63 mit Pegasus, vier mit Candiru und mindestens zwei Personen mit beiden

[583] El Pais, https://elpais.com/espana/catalunya/2022-05-30/el-juez-de-barcelona-archiva-de-forma-provisional-la-causa-por-el-espionaje-con-pegasus-a-torrent-y-maragall.html, 30. Mai 2022.
[584] Mission to Spain.
[585] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. Mai 2022.
[586] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. Mai 2022.
[587] El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html, 3. Mai 2022.
[588] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19. April 2022.
[589] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19. April 2022.

Programmen[590]. Mindestens 51 Geräte von Personen wurden erfolgreich infiziert[591]. Zu diesen angeblich entweder direkt oder indirekt überwachten Personen gehörten politische Persönlichkeiten, die für die Unabhängigkeit Kataloniens eintreten, wie der Minister für Wirtschaft und Arbeit und frühere Präsident des katalanischen Parlaments, Roger Torrent, der derzeitige Präsident der Esquerra Republicana de Catalunya (ERC) im Stadtrat von Barcelona und frühere Minister für auswärtige Angelegenheiten, institutionelle Beziehungen und Transparenz von Katalonien, Ernest Maragall sowie vier Mitglieder des Europäischen Parlaments. Da seit dem Beginn des Hackings und diesen Enthüllungen viel Zeit verstrichen ist, konnte eine Reihe von Zielpersonen aufgrund verschiedener Faktoren nicht identifiziert oder weiter untersucht werden, darunter eine Reihe von Zielpersonen, die das betreffende Telefon entsorgt haben[592].

330. Der spanische Premierminister Pedro Sánchez, die Verteidigungsministerin Margarita Robles und der Innenminister Fernando Grande-Marlaska wurden zwischen Mai und Juni 2021 mit Pegasus angegriffen[593]. Bisher liegen nur wenige Informationen über die Einzelheiten dieses Hackings vor, da sie von der Regierung angekündigt wurden und nicht das Ergebnis einer Untersuchung von CitizenLab oder eines anderen Recherchedienstes oder durch investigativen Journalisten waren und noch Gegenstand laufender Ermittlungen sind. Sánchez und Robles sind die Leiter der beiden Regierungsabteilungen, die den CNI, das für die Überwachung in Spanien zuständige Organ, beaufsichtigen. Die infizierten Geräte von Sánchez und Robles waren Regierungsgeräte und wurden gelegentlich auf Spähsoftware gescannt[594]. Grande-Marlaska wurde über sein privates Gerät infiziert[595]. Landwirtschaftsminister Luis Planas, der früher als Diplomat in Marokko tätig war, wurde ebenfalls mit Spähsoftware ins Visier genommen, eine erfolgreiche Infizierung fand jedoch nicht statt. Es wurde berichtet, dass die marokkanische Regierung möglicherweise für diese Angriffe verantwortlich sein könnte. Diese Informationen wurden jedoch nicht bestätigt[596].

331. Von den 65 Fällen wurden 18 als von den spanischen Behörden ins Visier genommen bestätigt, die Regierung äußerte sich jedoch nicht zu den 47 verbleibenden Personen[597]. Es bleibt unklar, ob die anderen Personen vom CNI mit einer gerichtlichen Anordnung ins Visier genommen wurden oder ob eine andere Behörde gerichtliche Anordnungen erhalten hatte, um sie rechtmäßig auszuspähen. Trotz der gerichtlichen Anordnungen für die Verwendung von Spähsoftware im Fall von 18 Personen wurden sie in der Folge nicht wegen einer Straftat angeklagt, die mit der genehmigten Verwendung von

---

[590] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 5.
[591] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 5.
[592] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, Seite 5.
[593] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. Mai 2022.
[594] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7. Mai 2022.
[595] La Razon, https://www.larazon.es/espana/20220510/gwxedc4drzhali5bqi4vbhk7kq.html.
[596] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7. Mai 2022.
[597] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. Mai 2022.

Spähsoftware zusammenhing. Zu den Zielpersonen, deren Überwachung angeordnet wurde, gehören der derzeitige Präsident von Katalonien, Pere Aragonès, der frühere Präsident und das derzeitige Mitglied des Europäischen Parlaments, Carles Puigdemont, sowie andere für die Unabhängigkeit eintretende Politiker und mit ihnen verbundene Personen[598]. Vorbehaltlich der im Gesetz enthaltenen Geheimhaltungs- und Vertraulichkeitsanforderungen hat sich Verteidigungsminister Robles auf das Gesetz über die Wahrung von Staatsgeheimnissen berufen, um die Gründe für die Überwachung dieser spezifischen Zielpersonen nicht erläutern zu müssen[599]. Die meisten der 65 katalanischen Zielpersonen standen zu irgendeinem Zeitpunkt in Kontakt mit den Mitgliedern der katalanischen Unabhängigkeitsbewegung, die außerhalb Spaniens leben. Einige der Zielpersonen befanden sich zum Zeitpunkt der Infizierung außerhalb Spaniens, unter anderem in Belgien, der Schweiz, Deutschland und Frankreich. Eine solche digitale Überwachung wäre in Deutschland rechtswidrig, es sei denn, diese wurde von den Bundesbehörden ausdrücklich gestattet.

332. Eine der Schlüsselgruppen, die – wie enthüllt wurde – zur Zielscheibe geworden ist, sind die unabhängigkeitsbefürwortenden katalanischen Mitglieder des Europäischen Parlaments. Jede und jeder von ihnen wurde entweder direkt oder indirekt anhand einer Methode, die von CitizenLab als relationale Zielbestimmung (relational targeting) bezeichnet wird, mit einer Spähsoftware gehackt[600]: Diana Riba i Giner, Jordi Solé, Carles Puigdemont und Clara Ponsatí. Das Mobiltelefon eines ehemaligen akkreditierten Assistenten von Clara Ponsatí wurde erfolgreich mit Pegasus infiziert. Im Fall von Antoni Comin, der den spanischen Staat beschuldigte, ihn während einer Anhörung des PEGA-Ausschusses ausspioniert zu haben, hat CitizenLab eingeräumt, dass seine Infizierung aufgrund einer fehlerhaften Zuordnung von Initialen irrtümlich gegenüber der falschen Person erfolgt war.

333. Das Telefon von Diana Riba i Giner, Mitglied des Europäischen Parlaments der Esquerra Republicana de Catalunya (ERC), wurde am 28. Oktober 2019, nur drei Monate nach ihrem Einzug ins Parlament, direkt mit der Spähsoftware Pegasus infiziert. Während eines Telefongesprächs mit ihrer Assistentin wurde die Kommunikation unterbrochen und ihre Mitarbeiterin hörte eine Aufnahme des Gesprächs, das sie gerade mit Riba i Giner geführt hatte. Der Zeitpunkt dieser Infizierung fiel direkt mit einem entscheidenden Gerichtsurteil über die katalanischen Separatisten zusammen, einer von ihnen Raül Romeva, Ehemann von Riba i Giner, der letztendlich eine 12-jährige Haftstrafe erhielt[601]. Riba i Giner schilderte bei einer Anhörung des PEGA-Ausschusses im Europäischen Parlament, dass zu dieser Zeit die meisten ihrer Telefongespräche das Gerichtsverfahren betrafen, und dass sie außerdem unzählige Besprechungen und Besuche bei den Gerichten absolvierte. Der zufällig erzielte Erfolg war in diesem Fall daher von enormer Bedeutung, auch für Romeva und Personen, die mit diesem

[598] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. Mai 2022.
[599] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html 5. Mai 2022.
[600] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, Seite 6.
[601] Untersuchungsausschuss zur Untersuchung des Einsatzes von Pegasus und gleichwertiger Spähsoftware, Anhörung von Frau Diana Riba i Giner, Mitglied des Europäischen Parlaments, Straßburg, 6. Oktober 2022.

wegweisenden Fall zu tun hatten[602].

334. Mitglied des Europäischen Parlaments Jordi Solé, ebenfalls vom ERC, der ebenfalls der ERC angehört, wurde laut ursprünglichem Bericht und Recherchen von CitizenLab sowohl am 11. als auch am 27. Juni 2020 gehackt[603]. Im selben Zeitraum wurden später jedoch fünf weitere Angriffe aufgedeckt[604]. Solé entdeckte nur zufällig, dass er mit Pegasus ausgespäht worden war, als er nach dem Erhalt einiger potenziell verdächtiger Nachrichten sein Telefon im Rahmen einer Dokumentation zur Überprüfung einreichte[605]. Ähnlich wie im Fall seiner Kollegin ist der Zeitpunkt dieses Angriffs bemerkenswert. Dieser fand während kritischer politischer Diskussionen über den vakanten Sitz von Oriol Junqueras statt, dem nicht gestattet wurde, sein Amt als Mitglied des Europäischen Parlaments anzutreten, während er in Spanien[606] inhaftiert war, und nur einen Monat bevor Solé ernannt wurde, um diesen Sitz im Juli 2020 zu übernehmen. Darüber hinaus gab es während der Zeit der Infizierungen laufende Diskussionen über die Parteistrategie und internationale Rechtsstreitigkeiten in Bezug auf ihre inhaftierten und im Exil lebenden Kollegen[607].

335. Carles Puigdemont, MdEP für JUNTS und ehemaliger Präsident Kataloniens, war über seine Ehefrau Marcela Topor, Mitarbeiter und eine Reihe mit ihm verbundener Personen zur Zielperson[608]. CitizenLab berichtet, dass insgesamt bis zu 11 Personen, die in engem Kontakt mit Puigdemont standen, ausgespäht wurden, darunter mindestens zwei bestätigte Infizierungen auf Topors Gerät am 7. Oktober 2019 und 4. Juli 2020[609].

336. Clara Ponsatí, MdEP für JUNTS und ehemalige Bildungsministerin Kataloniens, unterhielt Beziehungen zu einer Zielperson. Pol Cruz, ein Mitarbeiter des Europäischen Parlaments, wurde laut Bestätigung am 7. Juli 2020 infiziert[610].

337. Seit 2010 waren alle Ministerpräsidenten Kataloniens Angriffen mit Spähsoftware ausgesetzt, entweder während oder nach ihrer Amtszeit.[611] Unter den 65 Zielpersonen waren nicht weniger als 12 Mitglieder der Republikanischen Linken Kataloniens, einschließlich der Generalsekretärin der Partei, Marta Rovira, die laut CitizenLab im

---

[602]Untersuchungsausschuss zur Untersuchung des Einsatzes von Pegasus und gleichwertiger Spähsoftware, Anhörung von Frau Diana Riba i Giner, Mitglied des Europäischen Parlaments, Straßburg, 6. Oktober 2022.
[603] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 7
[604]Untersuchungsausschuss zur Untersuchung des Einsatzes von Pegasus und gleichwertiger Spähsoftware, Aussage des Mitglied des Europäischen Parlaments Jordi Solé, Straßburg, 6. Oktober 2022.
[605] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. April 2022.
[606]Untersuchungsausschuss zur Untersuchung des Einsatzes von Pegasus und gleichwertiger Spähsoftware, Aussage des Mitglied des Europäischen Parlaments Jordi Solé, Straßburg, 6. Oktober 2022.
[607] Politico, https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/, 9. Januar 2020.
[608] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 7.
[609] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 8.
[610] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S. 7.
[611] Artur Mas (nach seinem Ausscheiden aus dem Amt), Carles Puigdemont (Beziehungen zu einer Zielperson), Joaquim Torra (während seiner Amtszeit), Pere Aragones (infiziert während seiner Tätigkeit als Torras Vizepräsident). https://catalonia.citizenlab.ca/.

Juni 2020 mindestens zwei Mal gehackt wurde. Äußerst wichtig ist, dass sowohl Frau Gabriel als auch Frau Rovira zum Zeitpunkt ihrer Überwachung im Anschluss an die Unabhängigkeitserklärung Kataloniens nach dem Referendum im Jahr 2017 in der Schweiz lebten.

ZIVILE ZIELE, DARUNTER JOURNALISTEN, ANWÄLTE UND VERTRETER DER ZIVILGESELLSCHAFT

338. Jordi Domingo war einer der ersten katalanischen Aktivisten, der Berichten zufolge im Jahr 2020 zur Zielscheibe wurde. Obwohl er die Unabhängigkeit Kataloniens unterstützte und Mitglied der Katalanischen Nationalversammlung (ANC) war, wurde im Guardian berichtet, dass Domingo überzeugt war, irrtümlicherweise zur Zielperson geworden zu sein. Da er bei den Ereignissen im Jahr 2017 keine wesentliche Rolle gespielt hatte, war die eigentliche Zielperson seiner Ansicht nach ein Anwalt mit demselben Namen, der an der Erstellung eines potenziellen Verfassung Kataloniens mitgewirkt hatte[612].

339. Die Katalanische Nationalversammlung (ANC), eine katalanische zivilgesellschaftliche Organisation, die sich für die Unabhängigkeit Kataloniens einsetzt, war eine der ersten Organisationen, die im Vorfeld des katalanischen Referendums ins Visier genommen wurde, und war seitdem Opfer umfangreicher Angriffe[613]. Zu den sechs Zielpersonen in der ANC gehören zwei der früheren Präsidenten, Jordi Sánchez (2015-2017) und Elisenda Paluzie (2018-2022), deren Überwachung durch Spähsoftware per Gerichtsbeschluss genehmigt wurde, ebenso wie die des Experten digitale Abstimmungen und Dezentralisierung (Jordi Baylina), zwei Mitglieder des nationalen Vorstands (Arià Bayè und Sònia Urpí) und ein Mitglied einer Ortsgruppe (Jordi Domingo).

340. Die Geräte von Personen, die Jordi Cuixart, Präsident von Òmnium Cultural (bis Februar 2022) nahe standen, wurden infiziert, während er sich in Haft befand. Dazu gehörte Marcel Mauri, Vizepräsident der NGO, deren Überwachung mit Spähsoftware durch gerichtliche Anordnung genehmigt wurde.

341. CitizenLab entdeckte im Februar 2021 eine aktive Infektion mit Candiru auf dem Laptop von Joan Matamala, einem Aktivisten mit engen Verbindungen zu Politikern, die für die Unabhängigkeit Kataloniens eintreten[614]. Matamalas Überwachung mithilfe von Spähsoftware wurde durch gerichtliche Anordnung genehmigt. Candiru ist wesentlich schwieriger zu entdecken als Pegasus, und diese Entdeckung einer aktiven Infizierung ermöglichte es den Forschern von CitizenLab, die Muster besser zu verstehen. Anschließend wurden 16 weitere Infizierungen auf Matamalas Gerät entdeckt[615]. Microsoft hat in der Folge die Schwachstellen durch Updates behoben, aber es ist nicht möglich, die Anzahl der Candiru-Infektionen zu kennen, die unbemerkt

[612] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware, 13. Juli 2020.
[613] Citizen Lab's CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.
[614] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. April 2022.
[615] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. April 2022.

geblieben sind[616].

342. Mindestens drei renommierte Open-Source-Entwickler und -Unternehmer wurden mit Pegasus ausgespäht. Xavier Vives und Pau Escrich, Mitbegründer von Vocdoni, einem auf der Ethereum-Blockchain basierenden Open-Source-Protokoll für sichere, zensurresistente digitale Abstimmungen, wurden beide angegriffen. Vives wurde gezielt mit der Schadsoftware Candiru angegriffen, während Escrich sowohl mit Pegasus als auch mit Candiru angegriffen wurde[617]. Die Überwachung von Vives und Escrich mithilfe von Spähsoftware wurde durch eine richterliche Anordnung genehmigt.

343. Gonzalo Boye ist der Anwalt der ehemaligen Präsidenten Puigdemont und Torras[618]. In den fünf Monaten zwischen Januar und Mai 2020 wurde Boye durch Textnachrichten, die als Tweets von Organisationen der Zivilgesellschaft oder prominenten Nachrichtenagenturen ausgegeben waren, bis zu 18 Mal überwacht[619]. CitizenLab bestätigte mindestens eine erfolgreiche Infizierung am 30. Oktober 2020. Die Infizierung erfolgte nur 48 Stunden nach der Festnahme einer seiner Mandanten.[620] Dadurch, dass Boye zur Zielperson wurde, wurde die Rechtmäßigkeit eines Angriffs auf das das Anwaltsgeheimnis in Frage gestellt.

344. Elena Jimenez, die internationale Repräsentantin von Òmnium Cultural, und Jordi Bosch, der für institutionelle Beziehungen von Òmnium Cultural zuständige Anwalt, wurden beide mit Pegasus ausgespäht, während sie im juristischen Team von Jordi Cuixart tätig waren. Jimenez stand in ständigem Kontakt mit dem gesamten juristischen Team von Cuixart, einschließlich des internationalen Teams, das eine Klage vor dem EGMR vorbereitete. Bisher hat CitizenLab nur das zuletzt gekaufte Mobiltelefon von Jimenez untersucht, eine erfolgreiche Infizierung mit einer Zero-Click-Schadsoftware im Februar 2020 wurde jedoch bestätigt. Bosch, ein weniger öffentlich bekanntes Gesicht des juristischen Teams, wurde im Juli 2020 zur Zielscheibe, weniger als eine Woche bevor Cuixart eine mildere Form der Haft gewährt wurde und am selben Tag, an dem er zum ersten Mal im katalanischen Fernsehen im Namen von Òmnium auftrat.

345. Andreu van den Eynde i Adroer wurde am 14. Mai 2020 erfolgreich mit Pegasus infiziert.[621] Er wurde gehackt, während er als Anwalt seine Mandanten Raul Romeva und Oriol Junqueras in ihrem Verfahren vor dem Obersten Gerichtshof vertrat.

346. Auch das Gerät des Anwalts Jaume Alonso-Cuevillas wurde infiziert, während er katalanische Schlüsselfiguren wie Carles Puigdemont vertrat. CitizenLab war jedoch nicht in der Lage, das genaue Datum der erfolgreichen Infizierung festzustellen.

UNTERSUCHUNGEN UND GESETZESREFORMEN

---

[616] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. April 2022.
[617] https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#finding-catalans-targeted-with-candiru.
[618] https://catalonia.citizenlab.ca/.
[619] https://catalonia.citizenlab.ca/.
[620] https://catalonia.citizenlab.ca/.
[621] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. April 2022, S 10.

347. Nachdem die im Fall „CatalanGate“ enthaltenen Vorwürfe am 22. April 2022 bekannt geworden waren, begannen die spanischen Organe mit einem Kontrollverfahren, mit dem sichergestellt werden sollte, dass die Leitlinien für die Überwachung ordnungsgemäß angewandt wurden. Zu diesen Maßnahmen gehörte die Vorladung von Paz Esteban, Direktorin des CNI, vor dem Ausschuss für Staatsgeheimnisse, wie von Minister der Präsidentschaft Felix Bolaños am 5. Mai angekündigt, Sitzung der parlamentarischen Kontrolle der Regierung und des Verteidigungsministers am 26. und 27. April und die unabhängige Bewertung des Bürgerbeauftragten, die am 26. April eingeleitet und am 18. Mai abgeschlossen wurde. Die Verteidigungsministerin Margarita Robles, die gemäß dem Gesetz über die Wahrung von Staatsgeheimnissen zur Geheimhaltung verpflichtet ist, deutete an, dass die Maßnahmen als Reaktion auf die Handlungen derjenigen ergriffen wurden, die „die Verfassung verletzen, öffentliche Infrastrukturen übernehmen, öffentliche Unruhe stiften und [die] Verbindungen zu den politischen Führern eines Landes haben, das in die Ukraine eindringt“[622]. Die Regierungspartei (PSOE) und die drei großen Oppositionsparteien (PP, Vox und Ciudadanos) berichteten, dass die Direktorin zufriedenstellende Erklärungen zur Notwendigkeit und Rechtmäßigkeit der Überwachungsmaßnahmen durch Spähsoftware gegeben habe[623][624].

348. Der spanische Bürgerbeauftragte kam zu dem Schluss, dass ein Großteil der in Spanien durch den CNI durchgeführten Überwachungsmaßnahmen in vollem Einklang mit dem Gesetz erfolgt ist. Aufgrund seiner Empfehlungen für die Angemessenheit der parlamentarischen und gerichtlichen Kontrollen und im Hinblick auf die Aktualisierung der Gesetzgebung, der Stärkung der Garantien der gerichtlichen Kontrolle und der Sicherstellung eines Höchstmaßes an Achtung der Grundrechte des Einzelnen hat sich die spanische Exekutive verpflichtet:

1. Einleitung einer internen Untersuchung innerhalb des CNI,

2. Einleitung einer Untersuchung im Ausschuss für die Verwendung und Kontrolle der den geheimen Fonds des spanischen Kongresses zugewiesenen Mittel, und Durchführung einer Anhörung, in deren Rahmen der Direktor des CNI erscheinen würde, und

3. die Offenlegung gegenüber dem Ausschuss für die Verwendung und Kontrolle der den geheimen Fonds des spanischen Kongresses zugewiesen Mittel des Oberster Gerichtshofs; 18 Anordnungen zur Genehmigung der Durchsuchungen und die Freigabe von Dokumenten des CNI, die sich auf die ausgespähten Mitglieder der katalanischen Unabhängigkeitsbewegung beziehen, auf Antrag eines Richters,

4. Reform des spanischen Gesetzes von 1968 über Staatsgeheimnisse[625];

[622] El Pais, https://elpais.com/espana/2022-04-27/margarita-robles-sobre-el-espionaje-que-tiene-que-hacer-un-estado-cuando-alguien-declara-la-independencia.html, 27. April 2022.
[623] La Vanguardia, https://www.lavanguardia.com/politica/20220505/8245084/cni-aporta-autorizaciones-judiciales-parte-espionaje-catalangate.html, 5. Mai 2022.
[624] El Periodico de Espana, https://www.epe.es/es/politica/20220505/frente-comun-pp-vox-cs-13614030, 5. Mai 2022.
[625] El País, ‘El Gobierno inicia la reforma de la ley franquista de secretos oficiales’, 5. April 2021.

5. die Reform des Rechtsrahmens des CNI[626];

6. Verabschiedung einer neuen nachrichtendienstlichen Direktive, in der die nachrichtendienstlichen Ziele des CNI festlegt sind, und

7. Aktualisierung der nationalen Sicherheitsstrategie 2021 und des Cybersicherheitsplans.

349. Nachdem die Regierung behauptet hatte, die Pegasus-Spähsoftware sei zur Ausspähung von Ministern, darunter Premierminister Sánchez, eingesetzt worden, leitete der Oberste Gerichtshof Spaniens[627] eine eigene Untersuchung ein. Im Rahmen einer sogenannten Untersuchungskommission, die die Ausspähung untersuchen sollte, lud das Gericht den CEO der Firma NSO Group, die die israelische Spähsoftware Pegasus herstellt, und den Minister Felix Bolaños als Zeugen vor. Der Untersuchungsrichter befragte auch die frühere Direktorin des spanischen Geheimdienstes, Paz Esteban[628][629], sowie die Verteidigungsministerin und den Innenminister, deren Geräte ebenfalls gehackt worden waren. Der Gerichtshof[630] richtete ein förmliches Ersuchen um internationale Rechtshilfe an die israelische Regierung, in dem er um Informationen über „verschiedene Aspekte des Softwaretools“ bat. Darüber hinaus hob der Oberste Gerichtshof auch die Geheimhaltungsvorschriften für die mit dem Fall zusammenhängenden Dokumente und das Verbot, die Abhörung der Mobiltelefone von Premierminister Pedro Sánchez und Verteidigungsministerin Margarita Robles zu untersuchen, auf.

ABSCHLIEßENDE BEMERKUNGEN

350. Spanien verfügt über ein unabhängiges Justizsystem mit ausreichenden Schutzbestimmungen. Nach der Entdeckung der beiden Kategorien von Zielpersonen in Spanien bleiben jedoch einige Fragen offen, die durch rasche und tiefgreifende Reformen und deren wirksame Umsetzung beantwortet werden könnten. Die spanische Regierung arbeitet an Änderungen, um die Schwachstellen zu beseitigen. Hinsichtlich der Reform des CNI kündigte die spanische Regierung am 26. Mai 2022 an, den Rechtsrahmen des CNI reformieren zu wollen, doch bisher wurde kein Vorschlag vorgelegt. Am 1. August 2022[631] legte die Regierung Gesetzesänderungen zum Gesetz über die Wahrung von Staatsgeheimnissen vor. Die Regierung wartet derzeit auf die Stellungnahme des Staatsrates.

351. Die 47 im CitizenLab-Bericht erwähnten Zielpersonen, bei denen unklar ist, ob sie von

---

626 La Moncloa, ‘Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías’, 26. Mai 2022.
627 https://www.reuters.com/world/spanish-court-calls-ceo-israels-nso-group-testify-case-spying-with-pegasus-2022-06-07.
628 https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html.
629 https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations.
630 https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations.
631 https://www.mpr.gob.es/servicios/participacion/Documents/MAIN%20APL%20Informaci%C3%B3n%20Clasificada.pdf.

der CNI mit einem Gerichtsbeschluss ins Visier genommen wurden oder ob eine andere Behörde einen Gerichtsbeschluss erhalten hat, um sie rechtmäßig zu überwachen, kennen weder die Gründe, noch den Umfang oder die Akteure, die hinter den mittels Pegasus überwachten Zielpersonen stehen. Diese Personen sollten Zugang zu juristischer Unterstützung haben und eine Untersuchung sollte eingeleitet werden, um Klarheit bezüglich dieser Fälle zu schaffen.

352. Die Rechtmäßigkeit der 18 Fälle, in denen eine gerichtliche Anordnung ergangen war, wurde vom Bürgerbeauftragten geprüft und bestätigt, aber ihre Besonderheit, Angemessenheit, Außergewöhnlichkeit, Verhältnismäßigkeit und Notwendigkeit[632] kann nur von einem Gericht überprüft werden.

353. Im Allgemeinen verlaufen die Gerichtsverfahren der betroffenen Personen nicht so schnell wie erhofft, um für Transparenz und Zugang zu sinnvollen Rechtsbehelfen zu sorgen. Die Zusammenarbeit mit den Behörden ist hier entscheidend. Um mehr Klarheit zu schaffen und technisches Fachwissen beizusteuern, könnte Europol eingeladen werden und Unterstützung leisten, um sicherzustellen, dass ein ordnungsgemäßes kriminaltechnisches Verfahren befolgt wird.

I.F. Andere Mitgliedstaaten

DIE NIEDERLANDE

354. In der Koalitionsvereinbarung der niederländischen Regierung aus dem Jahr 2017 wurde festgehalten, dass es der niederländischen Polizei untersagt ist, Spähsoftware von Anbietern zu erwerben, die ihre Produkte „dubiosen Regimen“ zur Verfügung stellen, die später als „Länder, die sich schweren Verletzungen gegen die Menschenrechte oder humanitäres Völkerrecht schuldig gemacht haben“ bezeichnet werden. Vor dem Erwerb von Spähsoftware muss die niederländische Polizei den Anbieter fragen, ob er Spähsoftware an Länder geliefert hat, die von der EU oder den Vereinten Nationen sanktioniert wurden, und prüfen, ob das Land, in dem der Anbieter seinen Sitz hat, über ein Ausfuhrkontrollsystem verfügt, bei dem die Menschenrechte im Rahmen des Ausfuhrgenehmigungsverfahrens geprüft werden. Diese Prüfung wird regelmäßig wiederholt. Es sei darauf hingewiesen, dass diese Einschränkung lediglich für den Erwerb von Spähsoftware durch die Polizei zu gelten scheint. Die Nachrichtendienste werden nicht explizit erwähnt. Nach Regierungsinformationen nutzt die Polizei seit 2019 Hacking-Software, obgleich nicht erwähnt wird, welche Art von Software genutzt wird[633]. Die NSO Group und ihre Spähsoftware Pegasus würden die oben genannten Standards anscheinend nicht erfüllen, jedenfalls nicht vor der Verschärfung der israelischen Ausfuhrregelung im Dezember 2021[634]. In die Ausgaben für den Erwerb und die Nutzung des Spähsoftware-Systems wurde weder von der Polizei noch von den Nachrichtendiensten Einsicht gewährt.

355. In den Niederlanden hat 2018 ein neues Gremium (Toetsingscommissie inzet bevoegdheden, TIB) seine Arbeit aufgenommen, das für die Vorabprüfung der

[632] Article 588 a. i., Chapter IV, Criminal Procedure Act.
[633] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/23/ntwoorden-op-kamervragen-over-het-gebruik-van-hacksoftware-zoals-pegasus-in-nederland.
[634] https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021.

Rechtmäßigkeit der von der Regierung an die Nachrichtendienste erteilten Genehmigung zum Einsatz von Überwachungstechniken zuständig ist. Die Überwachung kann nicht fortgesetzt werden, wenn der TIB die Genehmigung für unrechtmäßig hält. Der TIB ergänzt das Hauptaufsichtsgremium, den Überprüfungsausschuss für die Nachrichtendienste und Sicherheitsdienste (Commissie Van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD). Der CTIVD überwacht die laufenden Überwachungstätigkeiten der Nachrichtendienste nach der Erteilung der Genehmigung und prüft Beschwerden.

356. Es sei darauf hingewiesen, dass die NSO Group von November 2014 bis Dezember 2016 dank zweier in den Niederlanden gegründeter Unternehmen, Shapes 1 BV und Shapes 2 BV, in den Bereichen „Finanzbeteiligungen“ und „Engineering und andere technische Planung und Beratung“ tätig sein konnte. Beide Unternehmen wurden nach zwei Jahren Betrieb wieder aufgelöst[635].

357. Am 4. Oktober 2022 wurde enthüllt, dass das niederländische Verteidigungsministerium im November 2019 einen Vertrag mit WiSpear unterzeichnen wollte, dem Unternehmen von Tal Dilian, der zuvor Cytrox erworben hatte, dem Hersteller der Spähsoftware Predator[636]. WiSpear hatte eine Ausschreibung des niederländischen Ministeriums gewonnen. Aus dem E-Mail-Austausch geht nicht eindeutig hervor, ob sie Predator oder ein anderes Produkt betrifft. Aus den offengelegten E-Mails, die zwischen dem zyprischen Ministerium für Energie, Handel und Industrie und WiSpear ausgetauscht wurden, geht hervor, dass ein Vertreter des niederländischen Verteidigungsministeriums das zyprischen Handelsministerium zwischen dem 13. und 15. November 2019, also nur wenige Tage bevor die Geschichte von dem Ausspähliefer wagen (spy van) von Dilian bekannt wurde, kontaktiert hatte, um Zusicherungen in Bezug auf WiSpear einzuholen. Dilian teilte der Vertreterin des zyprischen Handelsministeriums mit, dass er ihre sofortige Unterstützung in dieser Angelegenheit zu schätzen wisse, da die Frist für die Vertragsunterzeichnung bald ablaufe[637]. Es ist unklar, ob dieser Vertrag unterzeichnet wurde und ob dem niederländischen Verteidigungsministerium eine Spähsoftware zur Verfügung gestellt wurde.

358. In den Niederlanden befindet sich auch eine Tochtergesellschaft von Cognyte, die als Cognyte Netherlands B.V. eingetragen ist. Wie aus einem Auszug der niederländischen Handelskammer hervorgeht, ist der einzige Anteilseigner der niederländischen Tochtergesellschaft das in Zypern ansässige Unternehmen UTX Technologies. Wie im Kapitel über Zypern und die Spähsoftwareindustrie beschrieben, hat UTX Technologies in der Vergangenheit Spionage- und Ortungssysteme nach Bangladesch exportiert und Überwachungssysteme an EU-Mitgliedstaaten geliefert. Darüber hinaus war das israelische Unternehmen Verint – dem auch Cognyte vor seiner Ausgliederung im Jahr 2021 gehörte – der Hauptlieferant des Überwachungssystems für die niederländische Polizei[638]. Die Verbindungen zwischen der Polizei und diesem israelischen Lieferanten werden noch deutlicher, wenn man berücksichtigt, dass der ehemalige Polizeibeamte Robert van Bosbeek seit 2014 die Rolle des Direktors von

[635] Amnesty International, ‘Operating from the Shadows: Inside NSO Group’s Corporate Structure’, https://www.amnesty.org/en/documents/doc10/4182/2021/en/.
[636] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/.
[637] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/.
[638] Volkskrant: ‘Achterdeur in het nationale aftapsysteem van de politie, Israëli’s konden meeluisteren’.

Cognyte Netherlands B.V. übernommen hat[639]. Ein weiterer Direktor dieser niederländischen Tochtergesellschaft, David Abadi, ist auch der CFO der israelischen Cognyte Software Ltd, die mit dem Verkauf von Abhörsoftware an Myanmar in Verbindung gebracht wurde[640].

359. Am 2. Juni 2022 berichteten die Medien, dass der AIVD (niederländischer Allgemeiner Nachrichten- und Sicherheitsdienst, Algemene Inlichtingen- en Veiligheidsdienst) im Rahmen der Unterstützung der Polizei bei der Aufspürung des der schweren Kriminalität verdächtigen Ridouan T., der zum Hauptverdächtigen in mehreren Mordfällen im Zusammenhang mit organisierter Kriminalität, Drogenhandel und der Leitung einer kriminellen Vereinigung wurde und am 16. Dezember 2022 in Dubai festgenommen wurde, Pegasus eingesetzt hat[641]. Die niederländische Regierung lehnte eine Stellungnahme ab. Dies ist ein bemerkenswerter Fall, der eine genauere Betrachtung verdient. Die Informationen sickerten zu einer Zeit durch, als Pegasus und die NSO Group durch die Öffentlichkeit stark kritisiert wurden und durch die Aufnahme in die schwarze Liste durch das US-Handelsministerium finanziell belastet wurden. Die niederländische Erfolgsgeschichte der Festnahme einer Person, die seit Jahren zu den meistgesuchten Verbrechern gehörte, war eine willkommene positive Nachricht für das Unternehmen. Der Medienbericht stützt sich auf Aussagen von vier Quellen innerhalb des AIVD. Ihr Motiv für das Durchsickern der Informationen wird in dem Bericht nicht genannt. Auch scheint es keine Untersuchung dieser undichten Stellen gegeben zu haben, was die Frage aufwirft, ob die Informationen mit Billigung der AIVD-Leitung durchsickerten. Es ist jedoch höchst unwahrscheinlich, dass der AIVD zulassen würde, dass eine solche Geschichte ohne das Wissen und die Zustimmung der israelischen Behörden nach außen gelangt.

BELGIEN

360. In einem Interview mit *The New Yorker* enthüllte ein ehemaliger israelischer Geheimdienstmitarbeiter, dass die belgische Polizei Pegasus bei ihren Operationen einsetzt[642]. Daraufhin erklärte die belgische Polizei, „nicht über technische und/oder taktische Mittel zu kommunizieren, die für Ermittlungen und Einsätze verwendet werden“. Im September 2021 erwähnte Justizminister Vincent Van Quickenborne, dass Pegasus von den Geheimdiensten „auf legale Weise verwendet werden kann“, wollte aber nicht bestätigen, ob der belgische Geheimdienst ein Kunde von NSO ist oder Spähsoftware gegen Kriminelle einsetzt[643].

361. El Mahjoub Maliha, ein Menschenrechtsaktivist aus der Westsahara, der sich in Belgien aufhält, und Carine Kanimba, die Tochter des ruandischen politischen Aktivisten Paul Rusesabagina, wurden ebenfalls mit Hilfe der Pegasus-Software ausgespäht, während sie sich in Belgien aufhielten, sogar bei Treffen mit belgischen Regierungsvertretern. Die Angriffe mit Spähsoftware wurden höchstwahrscheinlich von den marokkanischen bzw. ruandischen Behörden oder in deren Auftrag durchgeführt. Ruanda wird außerdem

[639] Kamer van Koophandel: Bedrijfsprofiel - Cognyte Netherlands B.V. (34139430).
[640] Reuters: ‘Israel’s Cognyte won tender to sell intercept spyware to Myanmar before coup, documents show’.
[641] https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/.
[642] https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.
[643] https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spionagetool-pegasus/10329450.html.

beschuldigt, die Spähsoftware Pegasus eingesetzt zu haben, um im belgischen Exil lebende Kritiker ins Visier zu nehmen, darunter die prominenten Oppositionellen Placide Kayumba und David Batenga[644]. Der belgische Militärgeheimdienst ADIV fand außerdem heraus, dass Pegasus sehr wahrscheinlich von Ruanda auf dem Smartphone des belgischen Journalisten Peter Verlinden, einem Kritiker von Kagame, sowie auf dem Smartphone seiner Frau Marie Bamutese installiert worden war[645]. Zu den weiteren belgischen Zielpersonen, bei denen Spähsoftware zum Einsatz kam, gehören der ehemalige Premierminister Charles Michel und sein Vater Louis Michel (damals Mitglied des Europäischen Parlaments, ehemaliger Kommissar und Außenminister). Belgischen Medien zufolge steckte die marokkanische Regierung hinter den Angriffen[646].

DEUTSCHLAND

362. Zu den deutschen Stellen, die Hacking einsetzen und eingesetzt haben, gehören der Bundesnachrichtendienst, das Militär sowie Zoll und Polizei. Der BND ist die Behörde, die am häufigsten von der Möglichkeit des Hackens Gebrauch macht. Im Jahr 2009 hatte er bereits 2 500 Geräte überwacht[647].

363. In Deutschland gibt es einen rechtlichen Rahmen, der den Einsatz von Spähsoftware regelt. Seit 2008 werden der Polizei durch bundesrechtliche Vorschriften in Fällen des internationalen Terrorismus und zur Verhinderung von Terroranschlägen staatliche Hacking-Befugnisse eingeräumt[648]. Im Jahr 2017 ist ein neues Gesetz in Kraft getreten, mit dem es jeder Strafverfolgungsbehörde erlaubt ist, bei 42 Arten von auf staatliches Hacking zurückzugreifen. Zu diesen Straftaten gehören unter anderem die Stellung von betrügerischen Asylanträgen, Steuerhinterziehung und Drogendelikte[649]. Im Jahr 2021 hat der Bundestag den Gesetzentwurf der Bundesregierung „zur Anpassung des Verfassungsschutzrechts“ verabschiedet. Mit dieser Änderung werden staatliches Hacking für alle 19 deutschen Nachrichtendienste[650] legalisiert und die Kommunikationsanbieter zur Zusammenarbeit mit dem Staat bei Hacking-Aktivitäten verpflichtet[651].

364. Die Hacking-Gesetze in Deutschland werden häufig im Zusammenhang mit Straftaten gegen die sexuelle Selbstbestimmung, Kinderpornografie, der Bildung krimineller Vereinigungen und Mord gerechtfertigt. Die meisten Ermittlungen, bei denen die Polizei Hacking-Tools einsetzte, standen jedoch nicht im Zusammenhang mit den oben genannten Straftaten[652]. Der deutschen Polizei wurden gemäß der jüngsten Zahlen

---

644 https://www.ft.com/join/licence/88bec95c-78fd-4030-9526-a95fbdeb9da8/details?ft-content-uuid=d9127eae-f99d-11e9-98fd-4d6c20050229.
645 https://www.vrt.be/vrtnws/nl/2021/09/17/pegasus-spionageware-op-de-telefoon-van-journalist-peter-verlind/.
646 https://www.knack.be/nieuws/wereld/belgisch-slachtoffer-van-pegasus-spyware-mijn-leven-is-in-gevaar/; https://www.knack.be/nieuws/pegasus-project-macron-en-michel-in-het-vizier-van-marokko/.
647 European Parliament. Germany Hearing; https://www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html.
648 https://web.archive.org/web/20171008044948/https://www.gesetze-im-internet.de/bkag_1997/__20k.html.
649 https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0528.
650 https://www.bundestag.de/dokumente/textarchiv/2021/kw23-de-verfassungsschutzrecht-843408.
651 https://netzpolitik.org/2020/staatstrojaner-provider-sollen-internetverkehr-umleiten-damit-geheimdienste-hacken-koennen/.
652 European Parliament, Germany Hearing.

von 2020 48 Hacks genehmigt. Sie nutzte nur 22 Hacks, von denen keiner im Zusammenhang mit der Bekämpfung von Terrorismus und Mord stand[653].

365. Im September 2021 wurde berichtet, dass das deutsche Bundeskriminalamt (BKA) Pegasus Ende 2020 erworben hatte. Es ist wichtig, an dieser Stelle darauf hinzuweisen, dass das deutsche Recht zwischen zwei Formen des Einsatzes von Spähsoftware unterscheidet[654]: Zugriff auf alle Informationen (Online-Durchsuchung[655]) und Zugriff nur auf die Live-Kommunikation (Quellen-TKÜ[656]). Da die ursprüngliche Pegasus-Software auf alle Informationen auf einem Gerät zugreifen konnte und nicht nur auf die Live-Kommunikation, würde ihre Verwendung durch das BKA gegen das Gesetz verstoßen. Seit einem Grundsatzurteil des Bundesverfassungsgerichts aus dem Jahr 2008 muss jede Spähsoftware, die von Polizeibehörden eingesetzt wird, den für das BKA festgelegten Standards für die Telekommunikations- und Online-Überwachung entsprechen[657][658]. Das BKA ersuchte daher NSO darum, einen Quellcode zu schreiben, damit Pegasus nur auf die gesetzlich erlaubten Daten zugreifen kann. Zunächst weigerte sich NSO, dies zu tun[659]. Erst nach neuen Verhandlungen willigte NSO ein, sodass das BKA eine modifizierte Version erwarb[660]. Obwohl dies nicht öffentlich bestätigt wurde, bestätigte Martina Link, die damalige Vizepräsidentin des BKA, den Kauf einer modifizierten Version während einer nichtöffentlichen Sitzung des Innenausschusses im Bundestag[661]. Sie soll seit März 2021 im Einsatz sein. Bei der vom BKA gekauften Version waren bestimmte Funktionen gesperrt, um Missbrauch zu verhindern, obwohl unklar ist, wie dieser in der Praxis funktioniert. Das BKA hat einen Bericht über diese modifizierte Version verfasst, der jedoch als Verschlusssache eingestuft bleibt[662]. Das BKA hat zivilgesellschaftlichen Organisationen den Zugang zu den Verträgen mit den Spähsoftwarefirmen verweigerte, bis es gerichtlich dazu gezwungen wurde. Doch selbst dann wurden die Verträge nur in stark unkenntlich gemachter Fassungen freigegeben[663]. Trotz zweier Einladungen zum PEGA-Ausschuss war das BKA aufgrund von Terminproblemen nicht in der Lage, an Anhörungen teilzunehmen.

---

[653] Die Quellen-TKÜ (§ 100a StPO) wurde 25 Mal genehmigt und 14 Mal ausgeführt, die Online-Durchsuchung (§ 100b StPO) 23 Mal genehmigt und 8 Mal durchgeführt. Datenquelle: https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_TKUE_2020.pdf?__blob=publicationFile.

[654]https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.

[655]https://www.gesetze-im-internet.de/stpo/__100b.html.

[656]https://www.gesetze-im-internet.de/stpo/__100a.html.

[657] 'The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware', https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.

[658] Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf?__blob=publicationFile.

[659] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197.

[660] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197.

[661] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197.

[662] https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-prufbericht-zur-pegasus-software/.

[663] Testimony of Andre Meister, Country-Specific Hearing on Germany, Meeting of the Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, 14 November 2022. https://netzpolitik.org/2022/finfisher-vertrag-wir-haben-das-bka-verklagt-und-gewonnen/.

366. Im Oktober 2021 wurde ferner bekannt, dass der BND ebenfalls eine modifizierte Version von Pegasus gekauft hat, obwohl der Kauf als geheim eingestuft wurde[664]. Auf eine parlamentarische Anfrage hin teilte die Bundesregierung mit, dass der Einsatz von Pegasus nur in Einzelfällen und unter strengen rechtlichen Voraussetzungen nach der Strafprozessordnung (StPO), dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel-10-Gesetz) und dem Bundeskriminalamtgesetz (BKAG) zulässig ist, konnte aber aufgrund der Geheimhaltungsbedürftigkeit keine weiteren Angaben machen[665].

VERWENDUNG VON SPÄHSOFTWARE

367. In den Jahren 2012 und 2013 kauften sowohl das BKA als auch das LKA Berlin unabhängig voneinander FinSpy von FinFisher. Auch hier, genau wie im Fall von Pegasus, wies das BKA das Unternehmen angeblich an, die Spähsoftware FinFisher so zu entwickeln, dass sie nicht auf alle Daten auf einem Gerät zugreifen kann, sondern nur auf die Live-Kommunikation, damit sie mit den deutschen Gesetzen konform ist. Das BKA testete immer wieder neue Versionen der von FinFisher gelieferten Spähsoftware, um sie nur „rechtssicher und technisch sauber“ einzusetzen, und erst nach fünf Jahren, im Jahr 2018, genehmigte das Bundesinnenministerium ihren Einsatz. Dies geschah im selben Jahr, in dem der Einsatz der FinFisher-Software gegen Oppositionsparteien in der Türkei aufgedeckt wurde, wohingegen Deutschland seit 2015 keine Genehmigung für die Ausfuhr von Überwachungssoftware in Drittländer mehr erteilt hatte[666]. Der Vertrag zwischen FinFisher und der Berliner Polizei war zu diesem Zeitpunkt jedoch bereits ausgelaufen, sodass die Polizei in der Hauptstadt das Produkt nie eingesetzt hat. Das BKA hat nicht weiter Stellung dazu genommen, ob FinFisher bei seinen Einsätzen verwendet wurde oder ob der Vertrag noch gültig ist[667].

368. Im Jahr 2017 richtete der Bundesminister des Innern die Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) ein, um die Forschung und Entwicklung von Hacking-Tools durch die Regierung sowie den Ankauf von Hacking-Tools von kommerziellen Anbietern zu erleichtern[668]. Am 6. April 2022 wurde berichtet, dass ZITiS sich nach dem Insolvenzantrag des in Ungnade gefallenen Spähsoftware-Unternehmens FinFisher anderweitig nach verfügbaren Technologien umsehe[669]. Unter anderem wurde berichtet, dass sie sich seit 2019 fünfmal[670] mit dem italienischen Überwachungsunternehmen RCS Lab getroffen habe, aber es gab keinen Beweis für den Erwerb eines Tools von RCS Lab[671]. Darüber hinaus traf sich ZITiS mit

---

664 https://www.sueddeutsche.de/politik/pegasusprojekt-nso-pegasus-bundesnachrichtendienst-1.5433974.
665 https://dserver.bundestag.de/btd/19/322/1932246.pdf.
666 ‘The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware’, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.
667 https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/.
668 https://www.zitis.bund.de/DE/Home/home_node.html.
669 https://www.intelligenceonline.com/surveillance--interception/2022/04/06/after-finfisher-s-demise-berlin-explores-cyber-tool-options,109766000-art.
670 Answer to a parliamentary question by The Left Party MP Martina Renner https://dserver.bundestag.de/btd/20/038/2003840.pdf.
671 https://netzpolitik.org/2022/rcs-lab-hackerbehoerde-trifft-sich-mehrmals-mit-staatstrojaner-hersteller/.

dem österreichischen Anbieter DSIRF[672], den israelischen Anbietern Quadream[673] und Candiru[674] und bewertete deren Spähsoftware-Produkte.

369. Im Januar 2023 berichtete die *Tagesschau*, dass ZITiS auch mit Intellexa oder dessen Tochterunternehmen Cytrox in Kontakt stand, obwohl unklar ist, ob die Spähsoftware Predator letztendlich gekauft wurde. Der ehemalige Geheimdienstkoordinator Bernd Schmidbauer soll als Vertreter für die Produkte von Intellexa fungiert haben. Aus E-Mails aus November 2021 ist ersichtlich, dass Herr Schmidbauer in Kontakt mit dem ehemaligen Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik, Arne Schönbohm, stand, um einen Termin mit Intellexa zu vereinbaren. Im Februar 2022 nahm Schmidbauer auch Kontakt mit dem Präsidenten von ZITiS auf, um eine Präsentation von Intellexa zu erhalten. Zudem stand Schmidbauer in Kontakt mit dem Vizepräsidenten des Bundesamtes für Verfassungsschutz (BfV), was Berichten zufolge Anfang Juli 2022 zu einer Präsentation von Intellexa vor Beamten des BfV führte. Die Regierung äußerte sich nicht zu den Terminen, die sich aus den umstrittenen Lobbytätigkeiten von Herrn Schmidbauer ergeben[675]. Im Jahr 2021 hatte sich Schmidbauer auch mit Jan Marsalek getroffen, der mit DSIRF in Verbindung steht[676].

MALTA

370. Mehrere Schlüsselfiguren des Handels mit Spähsoftware haben ein Unternehmen auf Malta angemeldet oder einen maltesischen Pass erhalten, aber sie sind offenbar weder dort ansässig noch scheinen ihre Unternehmen dort aktiv zu sein. Bisher wurden einige wichtige Persönlichkeiten im Handel mit Spähsoftware identifiziert.

371. Tal Dilian ist israelischer Staatsbürger und war früher Mitglied der israelischen Armee. Er ist einer der Gründer von Intellexa und lebt in Zypern. Im Jahr 2017 erhielt er einen maltesischen Pass[677]. Er ist zudem Miteigentümer eines Unternehmens auf Malta mit dem Namen MNT Investments LTD[678].

372. Anatoly Hurgin ist ein russisch-israelischer Staatsbürger und ehemaliger israelischer Militäringenieur. 2015 erhielt er einen maltesischen Pass[679]. Er ist der Gründer der Ability Ltd., die zusammen mit der NSO Group an Pegasus arbeitete und die Netzwerkseite der Operationen von NSO betreute[680]. Zum Zeitpunkt der Beantragung

---

672 https://dserver.bundestag.de/btd/20/001/2000175.pdf#page=12.
673 https://dserver.bundestag.de/btd/20/001/2000104.pdf#page=29.
674 https://dserver.bundestag.de/btd/20/003/2000327.pdf.
675 https://www.tagesschau.de/investigativ/swr/predator-spionage-software-101.html. https://dserver.bundestag.de/btd/20/050/2005061.pdf.
676 https://www.tagesschau.de/investigativ/swr/wirecard-marsalek-schmidbauer-101.html.
677 Persons naturalised/registered as citizens of Malta 2017, published on 21 December 2018. https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf.
678 https://mlt.databasesets.com/company-all/company/73006; https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/.
679 https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429.
680 https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=543a981a3997; https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/.

seines maltesischen Passes ermittelten US-amerikanische und israelische Behörden bereits wegen verschiedener Straftaten gegen ihn[681]. Die Investigativjournalistin Daphne Caruana Galizia, die später im Oktober 2017 ermordet wurde, schrieb im August 2016 über ihn[682]. Im Jahr 2017 ermittelte die US-Börsenaufsichtsbehörde gegen die Ability Ltd. wegen angeblicher Lügen über den Zustand ihrer Finanzen und auch die NASDAQ-Notierung des Unternehmens wäre beinahe entzogen worden[683]. Hurgin ist Berichten zufolge auch Eigentümer eines Unternehmens in Litauen mit dem Namen UAB „Communication technologies“, das im Bereich „Verbindungs- und Telekommunikationsdienste“ tätig ist[684].

373. Direktor des in Malta ansässigen Unternehmens Baywest Business Europe Ltd.[685], war früherer ein Eigentümer und Mitarbeiter von Intellexa und war verwickelt in den Betrugsfall Piraeus/Libra[686];

374. Stanislaw Szymon Pelczar ist gesetzlicher Vertreter der Baywest Business Europe Ltd. mit Sitz in Malta und war früher Administrator bei Krikel. Seine Name tauchte in den Paradise Papers auf[687].

375. In Deutschland geborener amerikanischer Staatsbürger, der 2011 die neuseeländische Staatsbürgerschaft erworben hat, obwohl er dort keinen Wohnsitz hat. Er hat im Jahr 2022 (kurz nach der Ankündigung des gemeinsamen Start-ups von Kurz und Hulio) in Malta einen maltesischen goldenen Pass beantragt[688]. Er ist ein Gründer von PayPal und des umstrittenen Unternehmens Palantir (in Verbindung stehend mit dem Cambridge-Analytica-Skandal). Er unterstützt Donald Trump finanziell und ist der erste externe Investor bei Facebook. Er stellte Sebastian Kurz (der kürzlich ein Unternehmen mit Shalev Hulio, Ex-NSO, gegründet hat) als Strategen ein[689].

FRANKREICH

ZIELE IN FRANKREICH

376. Im Jahr 2021 deckte das Pegasus-Projekt mehrere Fälle von versuchten Hacks durch die Pegasus-Spähsoftware in Frankreich auf[690]. Dieser durchgesickerte Datensatz enthielt die Telefonnummer von Präsident Emmanuel Macron sowie die Telefonnummern von

---

[681] https://www.euractiv.com/section/all/short_news/mep-calls-out-malta-for-selling-passport-to-man-linked-to-pegasus-spyware/.
[682] https://daphnecaruanagalizia.com/2016/08/owner-israeli-phone-surveillance-hacking-software-intelligence-operation-buys-maltese-passporteu-citizenship/.
[683] https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/.
[684] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
[685] https://offshoreleaks.icij.org/nodes/55071906.
[686] https://www.haaretz.com/israel-news/tech-news/2022-04-19/ty-article/israeli-predator-spyware-found-in-phone-of-top-greek-investigative-reporter/00000180-6565-dc5d-a1cd-757f069c0000.
[687] https://offshoreleaks.icij.org/nodes/55071906.
[688] https://www.nytimes.com/2022/10/15/technology/peter-thiel-malta-citizenship.html.
[689] https://www.politico.eu/article/austria-former-chancellor-sebastian-kurz-palantir-technologies-silicon-valley-peter-thiel/.
[690] The Guardian, Pegasus spyware found on journalists' phones, French intelligence confirms.

14 Mitgliedern seines Kabinetts[691][692]. Die Ergebnisse forensischer Analysen des französischen Geheimdienstes haben bestätigt, dass die Telefone des Bildungsministers Jean-Michel Blanquer, der Ministerin für territorialen Zusammenhalt Jacqueline Gourault, des Landwirtschaftsministers Julien Denormandie, der Wohnungsbauministerin Emmanuelle Wargon und des Ministers für Überseegebiete Sebastien Lecornu mit der Pegasus-Spähsoftware infiziert waren[693]. Auch das Telefon des Parlamentsabgeordneten Adrien Quatennens war infiziert[694].

377. Das Verzeichnis, das dem Pegasus-Projekt vorlag, enthielt Berichten zufolge auch die Telefonnummern weiterer französischer Bürger, darunter Journalisten, ehemalige Politiker und deren Angehörige. Die Infizierung von Mobilgeräten des Direktors des Pariser Radiosenders TSF Jazz Bruno Delport, des ehemaligen Ministers Arnaud Montebourg und der Investigativjournalisten Edwy Plenel, Lénaïg Bredoux und eines namentlich nicht genannten Journalisten von France 24 durch Pegasus wurde von der französischen Computersicherheitsbehörde (Agence nationale de la sécurité des systèmes d'information) bestätigt[695]. Darüber hinaus wurde auch Claude Mangin – die Ehefrau von Naâma Asfari, einem saharauischen politischen Gefangenen in Marokko – mit Pegasus überwacht[696]. Außerdem wurde der in Paris ansässige Verteidiger mehrerer Polisorio-Aktivisten für die Sahara, Joseph Breham, ebenfalls mit Pegasus überwacht[697].

378. Hinter vielen der Angriffe auf Journalisten und Politiker in Frankreich scheint Marokko zu stecken[698], darunter auch marokkanische Journalisten, die im französischen Exil leben, insbesondere der Investigativjournalist Hicham Mansouri, der 2016 vor den ständigen Schikanen der marokkanischen Behörden floh, und der unabhängige Journalist Aboubakr Jamai, der Marokko 2007 verlassen hat[699].

379. Berichten zufolge wollte Frankreich selbst die Pegasus-Spähsoftware im Jahr 2021 kaufen. Zum Zeitpunkt der abschließenden Verhandlungen mit der NSO Group führten Enthüllungen über den angeblichen Einsatz der Spähsoftware gegen französische Regierungsbeamte zu einer abrupten Aussetzung des Geschäfts[700]. Das französische Außenministerium hat Gespräche mit der NSO Group dementiert[701].

380. In einer Sitzung des PEGA-Ausschusses am 9. Januar 2023 erklärte Serge Lasvignes – der Vorsitzende des Nationalen Ausschusses für die Kontrolle nachrichtendienstlicher Techniken –, dass die Entscheidung, den Einsatz von Pegasus in Frankreich nicht zu

[691] The Guardian, Spyware ‘found on phones of five French cabinet members’.
[692] Euractiv, France’s Macron targeted in project Pegasus spyware case.
[693] The Guardian, Spyware ‘found on phones of five French cabinet members’.
[694] https://www.google.com/url?q=https://www.bfmtv.com/politique/cible-par-le-logiciel-espion-pegasus-le-depute-insoumis-adrien-quatennens-annonce-deposer-plainte_AV-202107210122.html&sa=D&source=docs&ust=1674591349575339&usg=AOvVaw2rgujnaWzoVapS7ZbiH4-r.
[695] Haaretz, The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.
[696] Haaretz, The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.
[697] https://www.middleeasteye.net/fr/entretiens/pegasus-espionnage-maroc-france-macron-sahara-occidental-breham-avocat-mangin-algerie.
[698] Radio France, Projet Pegasus: le gouvernement et toute la classe politique française dans le viseur du Maroc.
[699] https://forbiddenstories.org/journaliste/hicham-mansouri/; https://forbiddenstories.org/journaliste/aboubakr-jamai/.
[700] MIT Technology Review, NSO was about to sell hacking tools to France. Now it’s in crisis.
[701] MIT Technology Review, NSO was about to sell hacking tools to France. Now it’s in crisis.

genehmigen, vor den Enthüllungen des Pegasus-Projekts getroffen worden sei. Laut Lasvignes nutzen die französischen Geheimdienste nur Überwachungsdienste, die in Frankreich entwickelt werden, um zu verhindern, dass ausländische Hersteller von Spähsoftware Zugang zu Informationen erhalten. Lasvignes präzisierte jedoch, dass die technische Direktion, die die französische Spähsoftware herstellt, in der Tat bestimmte Teile von nichtfranzösischen Unternehmen importiert[702].

381. Anträge auf Genehmigung der Überwachung einer Person müssen in Frankreich zunächst vom Generaldirektor der Dienststelle und dann vom Innenminister genehmigt werden. In letzter Instanz müssen alle Anträge vom Premierminister genehmigt werden. Derzeit werden in Frankreich 23 000 Personen überwacht, und jede Operation wurde vom Premierminister genehmigt. Möchte sich eine Zielperson erkundigen, ob sie überwacht wird oder wurde, wird ihr der Zugang zu ihren Akten mit Verweis auf die nationale Sicherheit verweigert. Die betroffene Person kann eine Überprüfung durch einen Richter beantragen. Der Richter kann jedoch nur entscheiden, ob die Überwachung rechtmäßig war oder nicht, kann aber die Zielperson nicht informieren, da dies unter die Geheimhaltung für die Zwecke der nationalen Sicherheit fällt[703]. Dies bedeutet, dass das Recht auf Rechtsbehelfe in der Praxis bedeutungslos ist, da die Beweislast bei der betroffenen Person liegt und es praktisch unmöglich ist, von den Behörden irgendwelche Beweise zu erhalten.

382. Laut einer Broschüre der ISS World aus dem Jahr 2013 waren das französische Innenministerium, das Verteidigungsministerium, Interpol und die Botschaft von Togo in Frankreich auf der ISS World 2012, auch bekannt als „The Wiretappers Ball“, als Teilnehmer vertreten. Darüber hinaus geht aus der Liste der ISS-Anbieter und Technologieintegratoren hervor, dass die folgenden französischer Spähsoftware-Firmen bei dieser Veranstaltung anwesend waren: Advantech, Amesys-Bull, AQSACOM France, Bertin Technologies, BreakingPoint, BULL, COFREXPORT, DataDirect Networks, Ercom, EXFO NetHawk, HALY3, Intersec, IP Solutions, OLEA Partners France, Scan & Target, Thales Communications & Security, Utimaco, VUPEN Security und WAHOUE AND PARTNERS[704].

SPÄHSOFTWARE-FIRMEN IN FRANKREICH

383. Frankreich ist Heimat verschiedener Spähsoftware-Unternehmen, von denen die bedeutendsten Nexa Technologies und Amesys sind. Nexa Technologies, Teil der Intellexa-Allianz von Tal Dilian, ist ein französisches Cyberverteidigungs- und Cyberinformationsunternehmen, das im Jahr 2000 gegründet wurde[705]. Nexa Technologies wird von ehemaligen Managern von Amesys geleitet. Amesys wurde 1979[706] gegründet und ist bekannt für den Verkauf eines Programms namens Cerebro, das in der Lage ist, die elektronische Kommunikation seiner Zielpersonen, wie E-Mail-Adressen und Telefonnummern, zu verfolgen[707].

---

[702] PEGA Committee hearing, 9 January 2022.
[703] PEGA Committee hearing, 9 January 2022.
[704] ISS World, Programme schedule for year 2013.
[705] Bloomberg, Nexa Technologies Inc.
[706] PitchBook, Amesys.
[707] Le Monde, Vente de matériel de cybersurveillance à l’Egypte: la société Nexa Technologies mise en examen.

384. Berichten zufolge verkaufte Amesys 2007 diese Technologie zur Telekommunikationsüberwachung an Libyen, wo sie dann vom Gaddafi-Regime zur Verhaftung und Folterung von Regimekritikern eingesetzt wurde. Nach Angaben von Telerama wurde Nexa gegründet, um die Überwachungssoftware umzubenennen und die Verkäufe von Amesys an das ägyptische Regime fortzusetzen[708]. Angeblich hatte Nexa Technologies im Jahr 2014 ein Abhörsystem unter dem Namen Eagle an das ägyptische Regime verkauft. Dieses System wurde im Zusammenhang mit der Inhaftierung und Folterung von politischen Gegnern des Al-Sissi-Regimes eingesetzt[709]. Eagle wurde von 2007 bis 2011 von Amesys bereitgestellt und gewartet[710].

385. Es wurden mehrere Klagen sowohl gegen Amesys als auch gegen Nexa Technologies eingereicht. Im Oktober 2011 reichten die FIDH und die LDH vor dem Pariser Gericht eine Klage gegen Amesys wegen angeblicher Verkäufe des Unternehmens an Libyen ein[711]. Im Sommer 2013 wurden fünf libysche Zielpersonen angehört, eine weitere libysche Zielperson wurde im Dezember 2015 angehört. In Folge neuer Beweise, durch die der Einsatz der Überwachungstechnologie von Amesys durch das Gaddafi-Regime untermauert wurde, wurde Amesys offiziell der Status als Zeuge mit Anspruch auf Rechtsbeistand wegen Beihilfe zur Folter zwischen 2007 und 2011 zugewiesen[712].

386. Im Jahr 2010 wurde Amesys von der französischen Computerfirma Bull übernommen. Im Jahr 2014 übernahm das damals von Thierry Breton geleitete Unternehmen Atos das Unternehmen Bull und damit auch Amesys[713]. Zum Zeitpunkt der Übernahme waren die zweifelhaften Aktivitäten von Amesys in Bezug auf den Handel mit autoritären Regimen bereits bekannt. Tatsächlich war bereits eine Beschwerde eingereicht worden.

387. Im Jahr 2017 wurde in einem investigativen Medienbericht der Verkauf von Überwachungssystemen an Ägypten im Jahr 2014 aufgedeckt, was zu einer Klage seitens der FIDH, LDH und des Cairo Institute for Human Rights Studies (CIHRS) gegen das Unternehmen führte[714][715].

388. Im Juni 2021 erhob das Pariser Gericht nach mehreren Klagen von Menschenrechtsorganisationen Anklage gegen vier Führungskräfte von Amesys und Nexa Technologies wegen des Verkaufs von Überwachungstechnologie an die Regierungen von Libyen und Ägypten[716]. Es ist besorgniserregend, dass zwischen der ersten Klage und dem Beginn des Gerichtsverfahrens ganze zehn Jahre vergangen sind. In der Zwischenzeit konnte Amesys seine Tätigkeit, einschließlich des oben erwähnten Verkaufs von Überwachungstechnologie an Ägypten, ungehindert fortsetzen.

389. Trotz dieser Kontroversen unterzeichnete die französische Agence Nationale des Titres Sécurisés (ANTS) im Oktober 2016 einen Vertrag im Wert von über 5 Millionen EUR

[708] ZDNet, Amesys and Nexa Technologies executives indicted.
[709] Trial International, Amesys (Nexa Technologies).
[710] ZDNet, Amesys and Nexa Technologies executives indicted.
[711] Trial International, Amesys (Nexa Technologies).
[712] Trial International, Amesys (Nexa Technologies).
[713] L'Obs, Amesys file un coup de main à l'agence en charge du fichier monstre.
[714] Le Monde, Vente de matériel de cybersurveillance à l'Egypte: la société Nexa Technologies mise en examen.
[715] ZDNet, Amesys and Nexa Technologies executives indicted.
[716] Amnesty, Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture.

mit Amesys für die technische Verwaltung der TES-Datenbank (die personenbezogene Daten und biometrische Daten aller französischen Bürgerinnen und Bürger enthält). Diese Entscheidung der französischen Behörden, Amesys, das damals schon für seine Praktiken bekannt war, in ein solches Projekt einzubeziehen, war Gegenstand von Kritik. Zwar sollte Amesys nicht die volle Kontrolle über die Systeme haben, die für die umstrittene TES-Datenbank verwendet wurden, aber es sollte die Projektmanager der Behörden unterstützen, die sich mit der TES-Datei befassen, sodass nicht ausgeschlossen werden konnte, dass Amesys Zugang zu personenbezogenen Daten haben würde. Der Direktor der ANTS war jedoch der Ansicht, dass es keine rechtlichen Einwände gegen eine Zusammenarbeit mit Amesys gebe[717].

390. In Frankreich werden Ausfuhrgenehmigungen von der Dienststelle für Güter mit doppeltem Verwendungszweck (Service des biens à double usage, SBDU) des Ministeriums für Wirtschaft, Industrie und digitale Angelegenheiten erteilt. Darüber hinaus prüft die interministerielle Kommission für Güter mit doppeltem Verwendungszweck unter dem Vorsitz des Ministeriums für Europa und auswärtige Angelegenheiten die sensibleren Güter mit doppeltem Verwendungszweck. Zum gegenwärtigen Zeitpunkt liegen keine Informationen über die Erteilung von Ausfuhrgenehmigungen durch die französische Regierung an Nexa Technologies vor.

IRLAND

391. Irland ist dank seiner Steuergesetze zu dem Mitgliedstaat geworden, in dem einige der wichtigsten in Skandale verwickelten Spähsoftware-Firmen registriert sind. Am 20. September 2022 enthüllte *The Currency*, ein irischer Verlag für investigativen Journalismus, dass sowohl Thalestris Limited, das Mutterunternehmen von Intellexa, als auch Intellexa selbst ihren Hauptsitz in Irland haben und bei einer Anwaltskanzlei in der Stadt Balbriggan registriert sind. Es ist bemerkenswert, dass der Antrag auf Eintragung von Thalestris Limited in Irland im November 2019 von einem Spezialisten für Unternehmensgründungen eingereicht wurde, nur 12 Tage nachdem die strafrechtliche Ermittlung der zyprischen Behörden gegen Dilian und sein Unternehmen WiSpear öffentlich bekannt wurden. Tal Dilian selbst, der Vorstandsvorsitzende von Intellexa, taucht in den irischen Unternehmensunterlagen nicht auf, aber Berichten zufolge wird seine zweite Ehefrau Sara Hamou als Direktorin sowohl von Thalestris als auch von Intellexa genannt[718].

392. Aus den von Thalestris veröffentlichten Jahresabschlüssen für den am 31. Dezember 2020 endenden Berichtszeitraum geht hervor, dass es zehn weitere Tochtergesellschaften in Griechenland, Zypern, der Schweiz und auf den Britischen Jungferninseln gibt und dass Thalestris keine Körperschaftssteuer zu zahlen hatte. Das Unternehmen nutzte eine Reihe von steuerlichen Bestimmungen, die auch von in Irland tätigen multinationalen Unternehmen angewandt werden, und verzeichnete daher technisch gesehen Verluste[719].

---

[717] L'Obs, Amesys file un coup de main à l'agence en charge du fichier monstre.

[718] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-inside-the-predators-irish-lair/.

[719] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/.

393. Die irische Regierung lehnte es ab, auf die Frage zu antworten, ob sie oder andere Strafverfolgungsbehörden von Thalestris oder Intellexa kontaktiert worden seien oder ob sie deren Dienste jemals in Anspruch genommen hätten, mit der Begründung, dass es „aus triftigen operativen und nationalen Sicherheitsgründen nicht angebracht wäre, sich zu den Einzelheiten der nationalen Sicherheitsvereinbarungen zu äußern, noch angebracht wäre, die Cybersicherheitsvereinbarungen des Ministeriums oder der staatlichen Ämter, Behörden und Stellen, die in den Zuständigkeitsbereich des Ministeriums fallen, offen zu legen“. Die irische Regierung lehnte es zudem ab, sich zu etwaigen irischen Verbindungen der von Thalestris und Intellexa hergestellten Spähsoftware zu äußern[720]. Es gibt keine öffentlich bekannten Beweise für Missbrauch von Spähsoftware in Irland.

394. Haaretz hat aufgedeckt, dass eine Firma namens GoNet Systems, die an der Bereitstellung von Wi-Fi-Infrastrukturdiensten auf dem Flughafen Larnaca beteiligt war und mit Dilians WiSpear in Verbindung stand und 2022 geschlossen wurde, auch Firmeneigentum in Irland hatte[721].

395. Im Januar 2023 wurde bekannt, dass der Justizausschuss des irischen Parlaments aufgrund eines Schreibens des Europaabgeordneten Barry Andrews die Existenz von Unternehmen in Irland untersuchen wird, die an der Herstellung von Spionageprogrammen beteiligt sind. Der Ausschuss erklärte, dass er die Angelegenheit in einer nichtöffentlichen Sitzung am 18. Januar erörtert und beschlossen habe, das Thema in sein Arbeitsprogramm für 2023 aufzunehmen[722].

396. Es sei darauf hingewiesen, dass das irische Gesellschaftsrecht ständig überprüft und regelmäßig aktualisiert wird, um die Transparenz der Unternehmensstrukturen zu steigern. Beispiele hierfür sind der Companies (Corporate Enforcement Authority) Act 2021, mit dem das Durchsetzungssystem aktualisiert wurde, und eine für 2023 erwartete Aktualisierung desselben sowie der Miscellaneous Provisions (Transparency and Registration of Limited Partnerships and Business Names) Bill 2023. Darüber hinaus kündigte die irische Regierung weitere Investitionen in das Nationale Cybersicherheitszentrum (NCSC) an, um das NCSC in die Lage zu versetzen, Cyberbedrohungen, die auf kritische Infrastrukturen und kritische Netze abzielen, aktiv aufzuspüren und mit verschiedenen Mitteln abzuwehren. Die Fähigkeit des NCSC, Vorfälle zu überwachen und darauf zu reagieren, wird durch die kontinuierliche Weiterentwicklung des Gemeinsamen Sicherheitsoperationszentrums (JSOC) sowie durch erweiterte Analyse- und Berichterstattungsmöglichkeiten weiter ausgebaut. Auch die Arbeiten an der Entwicklung einer Technologiestrategie für das NCSC mit externen Beratern gehen voran[723].

---

[720] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/.
[721] https://www.haaretz.com/israel-news/security-aviation/2022-09-20/ty-article-magazine/.highlight/as-israel-reins-in-its-cyberarms-industry-an-ex-intel-officer-is-building-a-new-empire/00000183-5a07-dd63-adb3-da173af40000?lts=1667755247674.
[722] https://www.irishtimes.com/politics/oireachtas/2023/01/29/justice-committee-to-investigate-controversial-spyware-technology-group-with-links-to-ireland/.
[723] https://www.kildarestreet.com/wrans/?id=2022-12-15a.199&s=cyber+security#g201.r.

LUXEMBURG

397. In Luxemburg sind neun Unternehmen ansässig, die direkt mit der NSO-Gruppe verbunden sind, wie Amnesty International im Juni 2021 aufdeckte und später seitens des luxemburgischen Außenministers Jean Asselborn bestätigt wurde[724]. Die Tatsache, dass die Namen der neun Unternehmen (wie Triangle Holdings SA, Square 2 SARL und Q Cyber Technologies SARL) die Verbindung zur NSO-Gruppe nicht sofort erkennen lassen, zeigt, wie undurchsichtige Geschäftsstrukturen in Luxemburg es den Unternehmen ermöglichen, völlig unbemerkt von der Öffentlichkeit zu operieren.

398. Nach den Enthüllungen von Amnesty über die neun NSO-Unternehmen in Luxemburg im Juni 2021 hat Außenminister Jean Asselborn an jedes von ihnen ein Schreiben gerichtet, in dem er sie aufforderte, alle Entscheidungen zu unterlassen, die zu einer illegalen Nutzung der Güter und Technologien führen könnten, die sie ihren Kunden zur Verfügung stellen. Laut der LuxTimes antwortete die NSO Group, dass sie ihre Spionagesoftware nur mit Zustimmung der israelischen Regierung aus Israel exportiere, aber Asselborn erklärte im Oktober 2021, dass er dies nicht überprüfen könne[725]. In jedem Fall, so der Minister, sei keines der neun Unternehmen befugt, Cyber-Überwachungsprodukte aus Luxemburg zu exportieren, da Luxemburg keine Exportlizenz erteilt habe[726]. Luxemburg werde unter keinen Umständen dulden, dass durch Exportgeschäfte aus Luxemburg zu Menschenrechtsverletzungen in Drittländern beigetragen werde, und werde gegebenenfalls sicherstellen, dass die notwendigen Maßnahmen ergriffen würden, um Menschenrechtsverletzungen abzuhelfen und zukünftige Verletzungen zu verhindern, so Asselborn[727]. Dennoch kann die NSO Group dank der in Luxemburg ansässigen Unternehmen wie Q Cyber Technologies, das für die Abwicklung von Rechnungen, Verträgen und Zahlungen von Kunden ihrer Software zuständig ist, weiterhin operieren[728]. Am 24. August 2022 wurde bekannt, dass die NSO Group mehr als die Hälfte ihres Umsatzes in den beiden Vorjahren in Luxemburg verbucht hatte, was deutlich macht, dass Luxemburg für die NSO Group ein wichtiges Geschäftszentrum ist[729].

399. Im Oktober 2021 bestätigte Premierminister Xavier Bettel, dass Luxemburg Pegasus aus Gründen der Staatssicherheit gekauft und eingesetzt hat[730].

ITALIEN

400. Bislang gibt es keine Berichte über den möglichen Kauf von Spähsoftware durch die italienischen Behörden. Es sind keine hochrangigen Fälle von Ausspähung bekannt

[724] https://www.amnesty.org/en/documents/doc10/4182/2021/en/.
[725] https://www.luxtimes.lu/en/luxembourg/government-cannot-verify-pegasus-export-claims-616eead9de135b9236b1efcc.
[726] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e.
[727] https://delano.lu/article/nine-nso-entities-in-luxembour.
[728] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e.
[729] https://www.luxtimes.lu/en/business-finance/pegasus-firm-nso-booked-most-sales-through-luxembourg-6303754ade135b9236e0870b.
[730] https://www.luxtimes.lu/en/luxembourg/tax-voting-rights-housing-watch-bettel-video-highlights-6176e835de135b923682378d.

geworden, obwohl die Telefonnummer des ehemaligen Ministerpräsidenten und Kommissionspräsidenten Romano Prodi auf der im Rahmen des Pegasus-Projekts veröffentlichten Liste gefunden wurde[731]. Als ehemaliger UN-Sonderbeauftragter für die Sahelzone hätte er ein interessantes Ziel für Marokko sein können, da er möglicherweise mit hochrangigen Persönlichkeiten in der Westsahara und Algerien vernetzt ist.

401. Die Spähsoftware-Firmen Tykelab und RCS Lab haben Italien als Standort für ihre Geschäfte gewählt.

402. Ein weiteres Unternehmen, das seit mindestens 2012 von Italien aus offensive Intrusion-Software anbietet, ist Hacking Team, inzwischen in Memento Labs umbenannt. Das Unternehmen erlangte Berühmtheit nach einem Hack, durch den Verkäufe an mehrere autoritäre Länder aufgedeckt wurden, die die Spähsoftware RCS für Angriffe auf politische Dissidenten, Journalisten und Menschenrechtsverteidiger einsetzten. Eine von Nichtregierungsorganisationen und VN-Ermittlern eingeleitete Untersuchung des Exports von RCS in den Sudan führte schließlich dazu, dass die italienischen Behörden aufgrund von Menschenrechtsbedenken einen „Auffangtatbestand“ einführten, sodass das Unternehmen für jeden Export eine Einzelgenehmigung einholen musste. Hacking Team verweigerte nicht nur die Zusammenarbeit im Rahmen der Ermittlungen, sondern nutzte auch seine engen Beziehungen zu hochrangigen Beamten aus Regierungskreisen, Nachrichtendiensten und Strafverfolgungsbehörden in Italien, um sich als wichtiger Faktor für die nationale Sicherheit zu positionieren, und übte schließlich Druck auf das Ministerium für wirtschaftliche Entwicklung aus, dem Unternehmen erneut eine globale Ausfuhrgenehmigung zu erteilen[732].

ÖSTERREICH

403. In der Antwort auf schriftliche Anfragen des österreichischen Parlaments erklärte die österreichische Bundesregierung, dass Österreich kein Kunde von NSO gewesen sei[733]. Der ehemalige Bundeskanzler Sebastian Kurz hat jedoch enge Beziehungen zum Gründer der NSO Group, und DSIRF, ein großer Spähsoftware-Anbieter, hat seinen Sitz in Österreich.

404. Nach seinem Rücktritt wurde Kurz als globaler Stratege für Thiel Capital eingestellt, das dem Milliardär Peter Thiel gehört[734]. Im Oktober 2022 gründeten Sebastian Kurz und Shalev Hulio (Gründer der NSO Group) ein Cybersicherheitsunternehmen namens Dream Security[735]. Obwohl Hulio im August 2022 als CEO der NSO Group

---

[731] https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.

[732] **1a** https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/;
https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/.

[733] Responses by former Minister of Interior Karl Nehammer to Member of National Council Nikolaus Scherak, 22 September 2021, reference 2021-0.580.421.

[734] https://www.bloomberg.com/news/articles/2021-12-30/billionaire-thiel-gives-austria-s-former-wunderkind-a-job.

[735] https://www.spiegel.de/netzwelt/web/sebastian-kurz-und-ex-nso-chef-gruenden-it-sicherheitsfirma-dream-security-a-4482132c-9faf-4be3-927a-86560ba28670.

zurückgetreten war, sind Dream Security und NSO durch verschiedene Persönlichkeiten und Geschäftsverbindungen eng miteinander verbunden. Einer der Investoren des Unternehmens, Adi Shalev, war ebenfalls ein früher Investor bei NSO. Gil Dolev ist ein weiteres Gründungsmitglied von Dream Security. Dolevs Schwester Shiri Dolev ist Präsidentin der NSO Group. Shalev Hulio hat zuvor eines der Unternehmen von Gil Dolev übernommen[736].

405. Im Juli 2022 nutzten Betreiber Spähsoftware des in Österreich ansässigen Unternehmens DSIRF, um sich in Anwaltskanzleien, Banken und Beratungsunternehmen in Österreich, Panama und Großbritannien einzuhacken. Laut Wissenschaftlern von Microsoft wurden von dem „Subzero"-Tool von DSIRF Zero-Day-Exploits genutzt, um auf vertrauliche Informationen wie Passwörter und andere Anmeldedaten zuzugreifen zu können[737]. Im Oktober 2022 erklärte das Bundesministerium für Arbeit und Wirtschaft, dass ihm keine Anträge auf Ausfuhrgenehmigungen durch DSIRF bekannt seien und dass in den letzten zehn Jahren keine Ausfuhranträge für „Intrusion-Software" gestellt worden seien[738]. Da keine Ausfuhrgenehmigung für die Ausfuhr von Software durch DSIRF vorlag, leitete die Staatsanwaltschaft Wien ein Ermittlungsverfahren wegen des Verdachts des rechtswidrigen Zugangs zu einem Computersystem nach österreichischem Recht ein.

ESTLAND

406. Berichten zufolge hat Estland ebenfalls Interesse am Kauf der Spähsoftware Pegasus der NSO-Gruppe gezeigt. Im Jahr 2018 fanden erste Verhandlungen zwischen Estland und der NSO-Gruppe statt, nach denen Estland eine Anzahlung auf das 30-Millionen-Dollar-Geschäft für die Überwachungssoftware leistete[739].

407. Ein Jahr später informierte jedoch ein russischer Verteidigungsbeamter Israel über die Absicht Estlands, die Pegasus-Spähsoftware im Zusammenhang mit russischen Telefonnummern einzusetzen. Diese Information veranlasste das israelische Verteidigungsministerium dazu, Estland die weltweite Ausspähung russischer Geräte zu verbieten, da dies den israelisch-russischen Beziehungen schaden würde[740]. Der Fall Estlands unterstreicht, dass es sich bei der Pegasus-Spähsoftware nicht nur um eine Überwachungswaffe handelt, sondern auch um ein politisches Instrument in den diplomatischen Beziehungen.

LITAUEN

408. Anatoly Hurgin, ein russisch-israelischer Staatsbürger, ehemaliger israelischer Militäringenieur und Mitentwickler von Pegasus zusammen mit NSO, ist Eigentümer eines Unternehmens in Litauen mit dem Namen UAB „Communication technologies",

---

[736] https://www.timesofisrael.com/former-nso-ceo-ex-chancellor-of-austria-establish-new-cybersecurity-startup/.
[737] Study entitled *'Pegasus and the EU's external relations',* European Parliament, Directorate-General for Internal Policies, Policy Department C – Citizens' Rights and Constitutional Affairs, 25 January 2023, p. 52; Microsoft (2022), Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits.
[738] https://www.parlament.gv.at/dokument/XXVII/AB/11698/imfname_1473647.pdf.
[739] The New York Times, 'Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia', 23. März 2022.
[740] The New York Times, 'Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia', 23. März 2022.

das im Bereich „Verbindungs- und Telekommunikationsdienste“ tätig ist[741]. Außerdem erwarb Hurgin 2015 einen maltesischen goldenen Pass[742].

BULGARIEN

409. In Bulgarien werden Ausfuhrkontrollen und Ausfuhrgenehmigungen für Erzeugnisse, die im Rahmen der EU-Dual-Use-Verordnung als Güter mit doppeltem Verwendungszweck eingestuft werden, vom Wirtschaftsministerium und insbesondere von der Interministeriellen Kommission für Ausfuhrkontrolle und Nichtverbreitung von Massenvernichtungswaffen kontrolliert[743]. Der derzeitige Minister für Wirtschaft und Industrie ist Nikola Stoyanov[744]. Die bulgarischen Behörden bestreiten, NSO Group oder ihren Tochtergesellschaften Ausfuhrgenehmigungen erteilt zu haben[745]. Der frühere Private-Equity-Eigentümer von NSO Group, Novalpina Capital, betonte jedoch, dass NSO-Produkte sowohl von Zypern als auch von Bulgarien aus in die EU exportiert werden[746][747][748]. Diese beiden Behauptungen sind widersprüchlich. Darüber hinaus ist laut Medienberichten einer der Server der Netzinfrastruktur, über die Pegasus-Angriffe durchgeführt werden, in einem bulgarischen Rechenzentrum untergebracht, das einem bulgarischen Unternehmen gehört. Dieses Unternehmen gehört NSO Group, Circles Bulgaria und Magnet Bulgaria, die von den Behörden Ausfuhrgenehmigungen erhalten haben. Von Bulgarien aus erbringt diese Tochtergesellschaft der NSO Group Forschungs- und Entwicklungsdienstleistungen für die zyprischen Tochtergesellschaften und exportiert Netzwerkprodukte an Regierungen[749]. Magnet ist derzeit nicht aktiv, Circles hingegen ist derzeit noch aktiv und hat eine Ausfuhrgenehmigung erhalten, die bis zum 25. April 2023 gültig ist[750].

410. Die Staatsanwaltschaft der Stadt Sofia hat im Februar 2022 eine Untersuchung eingeleitet, um festzustellen, ob durch staatliche Einrichtungen illegal die Spähsoftware Pegasus eingesetzt wurde, um bulgarische Bürger auszuspähen. Die Ermittlungen laufen derzeit[751]. Im Januar 2022 wurde im Rechtsstreit *Ekimdzhiev and Others* v *Bulgaria* ein Urteil gefällt, in dem der EMGR festgestellt hat, dass die bestehenden Gesetze in Bulgarien in Bezug auf die geheime Überwachung und die Vorratsdatenspeicherung und den Zugriff auf die Kommunikation nicht den Anforderungen der Konvention in Bezug auf die Rechtsqualität entsprechen, und er forderte die Regierung auf, die

---

[741] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
[742] https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.
[743] Republic of Bulgaria, Ministry of Economy and Industry, Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction.
[744] Council of Ministers of the Republic of Bulgaria.
[745] Politico, ‘Pegasus makers face EU grilling. Here’s what to ask them’, 21 June 2022.
[746] Amnesty International, ‘Novalpina Capital’s response to NGO coalition’s open letter’, 18. Februar 2019.
[747] Access Now, ‘Is NSO Group’s infamous Pegasus spyware being traded through the EU?’, 12. September 2019.
[748] https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/.
[749] Amnesty International, ‘Operating From the Shadows: Inside NSO Group’s Corporate Structure’.
[750] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuseruploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK.
[751] https://bnr.bg/en/post/101599684/sofia-city-prosecutor-s-office-investigates-possible-use-of-pegasus-spyware-in-bulgaria.

notwendigen Änderungen am nationalen Recht vorzunehmen, um die Verletzung zu beenden[752].

I.G. Organe der Union

DIE KOMMISSION ALS ZIEL

411. Am 11. April 2022 berichtete Reuters, dass Justizkommissar Didier Reynders und mindestens vier Kommissionsmitarbeiter im November 2021 mit Pegasus-Software angegriffen worden waren[753]. Am 23. November 2021 übermittelte Apple offizielle Benachrichtigungen an die Geräte von Kommissar Reynders und „weiteren Kommissionsbediensteten", in denen es hieß, sie seien „Ziel von staatlich geförderten Angreifern" geworden und ihre Geräte seien möglicherweise kompromittiert[754].

412. Im Anschluss an diese Enthüllungen wurde Kommissar Reynders eingeladen, am 30. Mai 2022 vor dem PEGA-Ausschuss zu sprechen, und beantwortete dessen Fragen auch schriftlich. Bereits am 19. Juli 2021, nach den Enthüllungen von Forbidden Stories und Amnesty International, setzte die Kommission ein „Spezialteam interner Experten" ein, „das mit einer internen Untersuchung beauftragt wurde", um „zu überprüfen, ob Pegasus Geräte von Kommissionsbediensteten und Mitgliedern des Kollegiums angegriffen hat"[755]. Die Kommission führte im September 2021 außerdem eine mobile „Endpoint Detection and Response"-Lösung (EDR) für alle Diensttelefone ein, die den Kommissionsdienststellen hilft, potenziell infizierte mobile Diensttelefone zu identifizieren.

413. Im Laufe der Untersuchung teilte die Kommission mit, dass Kontrollen „weder [...] vor oder nach diesem Datum [23. November 2021]" bestätigt hätten, dass die persönlichen oder dienstlichen Geräte von Kommissar Reynders kompromittiert worden seien. Die zuständigen Dienste der Kommission hätten auch Geräte anderer Bediensteter untersucht, die am gleichen Tag ähnliche Benachrichtigungen von Apple erhielten, aber auch bei keinem der untersuchten Geräte habe sich der von Apple aufgeworfene Verdacht bestätigt[756].

414. Jedoch räumte die Kommission in ihrem Schreiben vom 9. September 2022 ein, dass im Rahmen der andauernden Ermittlungen zu einem Angriff der Kommission mit Pegasus bei der Überprüfung verschiedener Geräte Indikatoren für Kompromittierungen gefunden worden seien. Die Kommission hat sich bisher weder öffentlich noch im PEGA-Ausschuss zu den Ergebnissen ihrer Untersuchung geäußert, da sie „den Gegnern die Untersuchungsmethoden und -fähigkeiten der Kommission offenbaren und somit die Sicherheit der Institution ernsthaft gefährden würde."[757]. Inoffizielle Berichte

[752] Ekimdzhiev and Others v Bulgaria, Application no. 70078/12, judgment of 11 January 2022, available at: https://hudoc.echr.coe.int/fre?i=001-214673.
[753] https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/.
[754] Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 July 2022; response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.
[755] Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 July 2022.
[756] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.
[757] https://pro.politico.eu/news/148627.

über mehr als 50 aufgedeckte Infektionen wurden von der Kommission nicht bestätigt.

415. Auf die Frage des PEGA-Ausschusses, welche(r) Akteur(e) hinter diesen Angriffen stecken könnte(n), antwortete die Kommission, dass es unmöglich sei, diese Hinweise mit absoluter Sicherheit einem bestimmten Täter zuzuordnen. Das übergreifende Thema, mit dem sich zwei der bekanntermaßen ins Visier genommenen Kommissionsbeamten, Kommissar Reynders und ein Mitglied des Kabinetts von Kommissarin Věra Jourová[758], beschäftigen, ist jedoch die Rechtsstaatlichkeit. In ihrer Antwort auf die Frage der PEGA nach einem möglichen Zusammenhang hat die Kommission abgelehnt, weitere Informationen über die Anzahl der möglicherweise kompromittierten Abteilungen, über die Berufe der betroffenen Mitarbeiter oder andere Informationen, die für die Arbeit des PEGA-Ausschusses von Interesse wären und den Ursprung des Angriffs bestimmen könnten, mitzuteilen, und erklärte, sie verfüge „nicht über genügend Informationen, die es uns erlauben, endgültige Schlussfolgerungen über einen Zusammenhang zwischen Geolokalisierung und einem möglichen Versuch der Geräteinfektion über Pegasus zu ziehen.“[759].

416. In Anbetracht der obigen Ausführungen sind mehrere Probleme zu erkennen. Erstens hat die Kommission kein ausreichendes Bewusstsein und Verständnis für die enormen politischen Risiken gezeigt, die damit verbunden sind, mithilfe von Spähsoftware überwacht zu werden. Jeder Hacking-Versuch, ob erfolgreich oder nicht, auf die Kommission bzw. auf ein Mitglied der Kommission ist eine sehr ernst zu nehmende politische Tatsache, die Auswirkungen auf die Integrität der demokratischen Entscheidungsprozesse hat. Im Rahmen ihrer Interaktion mit dem PEGA-Ausschuss erklärte die Kommission wiederholt, dass der Versuch, Kommissar Reynders Gerät mit Pegasus-Software zu hacken, nicht erfolgreich gewesen sei. Wie die Kommission jedoch selbst feststellte, führten „mehrere Gerätekontrollen [der Geräte der Mitarbeiterinnen und Mitarbeiter] zur Entdeckung von Hinweisen auf eine Kompromittierung“, worüber es keine weitere Mitteilung gab. Dies scheint darauf hinzudeuten, dass die Kommission die Tragweite des Angriffs auf eine EU-Institution herunterspielt.

417. Zweitens reichten die IT-Kapazitäten und -Fähigkeiten offenbar nicht aus, um Kommissionsmitglieder und Mitarbeiterinnen und Mitarbeiter vor Angriffen zu schützen oder ihre Cybersicherheit zu beaufsichtigen und zu überprüfen. Obwohl die Kommission neue Maßnahmen wie die EDR-Lösung auf allen Telefonen der Kommission eingeführt hat und kontinuierlich mit CERT-EU[760] zusammenarbeitet, ist aufgrund der fehlenden Informationen, die PEGA von der Kommission erhalten hat, unklar, inwieweit die Maßnahmen der Kommission zur Analyse früherer Spähsoftware-Angriffe erfolgreich waren und inwieweit die ergriffenen Maßnahmen in Zukunft ausreichend sein werden.

418. Drittens hat die Kommission der belgischen Polizei die Meldungen oder die Anzeichen für eine Kompromittierung nicht offiziell zur weiteren Untersuchung gemeldet, sondern im Rahmen ihrer „regelmäßigen Zusammenarbeit“ lediglich „technische Einzelheiten“ mit der belgischen Polizei besprochen. Die Kommission erklärte, dass Mitteilungen

[758] https://pro.politico.eu/news/148627.
[759] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.
[760] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.

dieser Art jeden Tag mehrfach bei den zuständigen IT-Abteilungen der Kommission eingehen würden und daher nicht offiziell bei der Polizei gemeldet werden müssten. Nach Aussagen der Kommission habe sie keine Folgemaßnahmen seitens der Strafverfolgungsbehörden veranlasst, da die Benachrichtigung von Apple nicht eine definitive Infizierung zum Gegenstand gehabt habe, sondern lediglich den möglichen Versuch einer Schadsoftware, das entsprechende Gerät anzugreifen[761].In anderen Fällen, z. B. in Spanien und Frankreich, wurden jedoch gegen Minister und Staats- und Regierungschefs strafrechtliche Ermittlungen hinsichtlich des Einsatzes von Spähsoftware eingeleitet. Spyware wird hauptsächlich von staatlichen Akteuren unter Berufung auf Gründe der nationalen Sicherheit verwendet. Die Kommission behauptet, dass einige Aspekte betreffend die nationale Sicherheit nicht in den Zuständigkeitsbereich der Kommission fallen[762], aber sie bleibt eine Erklärung schuldig, inwiefern Mitglieder und Bedienstete der Kommission ein nationales Sicherheitsrisiko darstellen könnten.

419. Viertens bedeutet die Tatsache, dass die Kommission dem PEGA weder *unter Ausschluss* der Öffentlichkeit aussagekräftige Informationen über die Ausrichtung der Kommission noch allgemein mit grundlegenden Informationen im Zusammenhang mit der Untersuchung zur Verfügung gestellt hat, dass das Parlament keine ordnungsgemäße demokratische Kontrolle ausüben konnte. Die Kommission sollte neu bewerten, welche Informationen sie offenlegen kann, um eine sinnvolle parlamentarische Kontrolle zu ermöglichen.

ANGRIFFE AUF MITGLIEDER DES EUROPÄISCHEN RATES, DES RATES UND DER KOMMISSION

420. Nicht nur ein derzeitiges Kommissionsmitglied und andere Kommissionsbedienstete wurden ins Visier genommen, sondern auch Regierungschefs, Minister und ein ehemaliges Kommissionsmitglied wurden angeblich mit Spähsoftware von außerhalb und innerhalb der Union ins Visier genommen.

421. Die Telefonnummer des französischen Präsidenten Macron erschien auf der Pegasus-Projektliste potenzieller Ziele, und die spanische Regierung bestätigte, dass die Telefone des spanischen Premierministers Pedro Sánchez, der Verteidigungsministerin Margarita Robles und des Innenministers Fernando Grande-Marlaska mit der Spähsoftware Pegasus infiziert waren, angeblich von außerhalb der Union.

422. Laut der griechischen Zeitung Documento, die eine umfangreiche Liste von Personen veröffentlichte, auf deren Geräten angeblich Spuren von Predator gefunden wurden, wurden[763] Dimitris Avramopoulos, der von 2014 bis 2019 EU-Kommissar war, und mehrere derzeitige Regierungsminister, darunter der Außenminister und der Finanzminister, mit Spähsoftware ins Visier genommen. . Es ist nicht klar, ob die angeblichen Hacking-Versuche auf Avramopoulos während seiner Zeit als Mitglied der Kommission stattgefunden haben, noch ist klar, wer dahinter steckte. Auf der langen Liste der Zielpersonen stehen jedoch auch viele griechische Politiker sowohl aus der

[761] Antwortschreiben der Kommissionsmitglieder Hahn und Reynders vom 9. September 2022 an den PEGA-Ausschuss.
[762] Antwortschreiben der Kommissionsmitglieder Hahn und Reynders vom 25. Juli 2022 an die Berichterstatterin.
[763] Documento, edition of 6 November 2022.

Regierungspartei als auch aus der Opposition.432. Diese bestätigten und mutmaßlichen Infizierungen und Hacking-Versuche zeigen, dass die derzeitigen Staats- und Regierungschefs und die derzeitigen oder ehemaligen Kommissionsmitglieder, einschließlich ihrer Kommunikation mit Kollegen, von außerhalb oder innerhalb der Union ins Visier genommen werden könnten, während sie Mitglieder des Europäischen Rates, des Rates und der Kommission sind. Daher könnte ein einziges infiziertes Telefon auch die Informationen der Organe ernsthaft gefährden, einschließlich der Informationen, die während der Sitzungen der Kommission und des Rates in Echtzeit ausgetauscht werden.

I.H. Drittländer

423. Im folgenden Abschnitt wird beleuchtet, inwieweit mit dem Einsatz von Pegasus oder ähnlicher Überwachungs- und Spähsoftware unter unmittelbarer oder mittelbarer Beteiligung von Einrichtungen mit Verbindungen zur EU zur illegalen Ausspähung von Journalisten, Politikern, Strafverfolgungsbeamten, Diplomaten, Rechtsanwälten, Geschäftsleuten, Akteuren der Zivilgesellschaft, Menschenrechtsverteidigern und anderen Akteuren in Drittländern beigetragen wurde. Dazu gehört auch die Frage, inwieweit der Einsatz von Spähsoftware zu Menschenrechtsverletzungen geführt hat, die im Hinblick auf die Ziele der Gemeinsamen Außen- und Sicherheitspolitik der EU Anlass zu ernster Besorgnis geben, und ob mit einem solchen Einsatz gegen die in Artikel 21 EUV und in der Charta verankerten Werte verstoßen wurde, auch unter gebührender Berücksichtigung der Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte und anderer in den internationalen Menschenrechtsnormen verankerter Rechte.

424. Von den Drittländern, die in den Einsatz von Spähsoftware involviert sind, hat der PEGA-Ausschuss Israel und Marokko besondere Aufmerksamkeit gewidmet, und zwar im Rahmen einer Anhörung und einer Reise nach Israel im Juli 2022 und einer Sitzung zu Marokko im Februar 2023 im Zuge einer Anhörung zur Geopolitik von Spähsoftware. Darüber hinaus wurde eine Anhörung im August 2022 zum Teil Ruanda gewidmet, während der auch Carine Kanimba, die ein Ziel von Pegasus war zu Wort kam.

ISRAEL

425. Der PEGA-Ausschuss besuchte Israel im Juli 2022. Der Hauptzweck der Reise war es, sich mit dem Hersteller der Pegasus-Spähsoftware, dem israelischen Unternehmen NSO Group, zu treffen. Die PEGA-Delegation erfuhr, dass die NSO Group Spähsoftware mit Ausfuhrgenehmigungen der israelischen Regierung an 14 EU-Regierungen verkauft hat. Sie erörterten den Missbrauch von Söldner-Spähsoftware und deren Auswirkungen auf die Demokratie, die Rechtsstaatlichkeit und die Grundrechte in der EU. Der Ausschuss traf auch Vertreter der Regierung, der Knesset, Sachverständige und Mitglieder der Zivilgesellschaft. Dieser Besuch verdeutlichte die Unwirksamkeit bestehender Schutzmaßnahmen gegen den Missbrauch von Spähsoftware und die Notwendigkeit einer viel strengeren Regulierung des Verkaufs, des Kaufs und der Verwendung von Spähsoftware durch die Europäische Union. Der Bereich der Cyberüberwachung muss

wirksam reguliert werden, um den Missbrauch von Spähsoftware in Zukunft zu verhindern.

426. Israels geopolitische und sicherheitspolitische Situation hat seine Regierung und den privaten Sektor dazu veranlasst, nachrichtendienstliche Instrumente zu entwickeln, die die Cybersicherheitskapazitäten des Landes erweitern würden, insbesondere im Hinblick auf seine Verteidigung. Im Laufe der Jahre hat sich Israel zu einem der weltweit führenden Hersteller von fortschrittlichen Überwachungstechnologien und Spähsoftware entwickelt, da es über beträchtliche Expertise bei der Entwicklung von Tools zur Sammlung von nachrichtendienstlichen Informationen verfügt. Die Branche exportiert ihre Produkte weltweit. In einer vom Europäischen Parlament in Auftrag gegebenen und 2023 unter dem Titel „Pegasus und die Außenbeziehungen der EU“ (Pegasus and the EU's external relations) veröffentlichten Studie wurde festgestellt, dass „die Spyware-Industrie für Exportländer eine lukrative Einnahmequelle und ein Hebel für diplomatischen Einfluss sein kann“[764]. Dies wird auch durch Medienberichte bestätigt, in denen Experten die Nützlichkeit von Pegasus bei der Aufnahme diplomatischer Beziehungen, z. B. mit den Golfstaaten, hervorheben[765].

427. Neben den strategischen Gründen im eigenen Land hat sich Israel erfolgreich als innovative Start-up-Nation profiliert und verfügt über Unternehmen, die über die fortschrittlichsten Technologien in diesem Bereich verfügen, wie NSO, Cellebrite, Candiru, QuaDream und Intellexa. Die Verkäufe der Branche werden insgesamt auf mindestens 1 Milliarde US-Dollar jährlich[766] geschätzt, was etwa 0,6 % der israelischen Exporte entspricht[767]. Israels Verteidigungskräfte und Geheimdienste, insbesondere seine Cybersicherheitsabteilung namens Unit 8200, haben eine wesentliche Rolle in Israels erfolgreicher Spähsoftware-Branche gespielt und Firmen unterhalten enge Beziehungen zur Behörde. Laut einer Studie aus dem Jahr 2018 waren 80 % der 2 300 Menschen, die Israels 700 Cybersicherheitsunternehmen gründeten, ehemalige Mitarbeiter der Geheimdienste der israelischen Streitkräfte. Eine der prominentesten Persönlichkeiten in der Branche ist der Eigentümer und Gründer von Intellexa, Tal Dilian (siehe Abschnitt zu Intellexa und Tal Dilian)[768].

428. Israelische Spähsoftware-Unternehmen haben Überwachungstechnologie in die ganze Welt verkauft, einschließlich an Mitgliedstaaten der EU und an autoritäre Golfstaaten. Laut der Zeitung Haaretz wurde der Verkauf von Pegasus als diplomatisches Druckmittel verwendet und erleichterte die Verhandlungen über die Aufnahme offizieller diplomatischer Beziehungen zu Marokko, Bahrain und offiziell auch zu den

[764] 'Pegasus and the EU's external relations', Europäisches Parlament, Generaldirektion Interne Politikbereiche, Fachabteilung C – Bürgerrechte und konstitutionelle Angelegenheiten, 25. Januar 2023.
[765] https://www.france24.com/en/livenews/20210719-pegasus-scandal-showsrisk-of-israel-s-spy-tech-diplomacyexperts.
[766] https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.
[767] https://en.globes.co.il/en/article-israels-exports-rise-sharply-in-2022-1001433699#:~:text=According%20to%20a%20conservative%20estimate,a%20then%20record%20%24144%20billion.
[768] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106.

Vereinigten Arabischen Emiraten im Rahmen des Abraham-Abkommens[769]. Der Verkauf von Spähsoftware an autoritäre Regime wurde kritisiert, vor allem im Zuge des Pegasus-Projekts. Infolgedessen verschärfte die israelische Regierung im Dezember 2021 die Ausfuhrbestimmungen für Instrumente der elektronischen Kriegsführung. Angesichts der geplanten Justizreform in Israel werden Berichten zufolge vielen israelischen Technologieunternehmen Anreize von Griechenland, Zypern und Portugal angeboten, ihre Geschäfte in diese Länder zu verlagern. Medienberichten zufolge bieten diese drei Länder israelischen Technologieunternehmen Steuererleichterungen an, während Griechenland Berichten zufolge eine beschleunigten Prozess zum Erhalt der Staatsbürgerschaft bereitstellt[770].

429. Experten zufolge schafft Israel mit seiner Bereitschaft, neue Überwachungssysteme an Palästinensern in den besetzten Gebieten zu testen, Anreize für ein Geschäftsmodell in der Überwachungsbranche, wovon auch NSO profitiert hat[771]. Infolgedessen tragen Länder, die in der Praxis erprobte („field trained“) Spähsoftware aus Israel kaufen, zu Menschenrechtsverletzungen in den vorgenannten Regionen bei. Mitgliedstaaten der EU, die zu den renommiertesten Kunden der NSO Group zählen, stehen somit im direkten Widerspruch zur außen- und sicherheitspolitischen Agenda der EU hinsichtlich der Unterstützung der Menschenrechte und der Demokratie[772].

430. Die Pegasus-Spähsoftware der NSO Group wurde eingesetzt, um die palästinensische Zivilgesellschaft ins Visier zu nehmen, darunter sechs palästinensische Menschenrechtsverteidiger[773]. In den Fällen von Ubai Al-Aboudi, Exekutivdirektor des Bisan Center for Research and Development, und Salah Hammouri, ein Franzose mit doppelter Staatsbürgerschaft, Rechtsanwalt und Wissenschaftler, der für die Organisation „Addameer Prisoner Support“ und Menschenrechtsorganisationen tätig ist, scheint der Einsatz von Überwachungs- und Spähsoftware zu Administrativhaft geführt zu haben. Die Überwachung aller sechs Personen fällt mit der höchst umstrittenen Einstufung von sechs palästinensischen Menschenrechtsorganisationen als „terroristisch“ zusammen, was zu einen internationalen Aufschrei führte, der die Entscheidung der israelischen Regierung verurteile. Dieser Fall der Überwachung palästinensischer Menschenrechtsverteidiger ist noch mehr der Beweis für die mangelnde Durchsetzung der Menschenrechtspolitik der NSO[774], mit der das Unternehmen seine Legitimität und Glaubwürdigkeit beim Verkauf an EU-Mitgliedstaaten gestärkt hat.

---

[769] Haaretz (2022) ‘Netanyahu Used NSO’s Pegasus for Diplomacy’, https://www.haaretz.com/israelnews/2022-02-05/tyarticle/.premium/netanyahu-used-nsospegasus-for-diplomacy-now-he-blames-itfor-his-downfall/0000017f-e941-dc91- a17f-fdcd55c80000.

[770] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/ ; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106.

[771] PEGA Mission to Israel, 18 to 20 July 2022.

[772] Im Einklang mit den meisten Ergebnissen des Jahresberichts der Kommission für 2021 über die Anwendung der Charta der Grundrechte der EU mit dem Titel „Schutz der Grundrechte im digitalen Zeitalter“ (Protecting Fundamental Rights) ist die EU verpflichtet, die Arbeit von Menschenrechtsverteidigern im Internet zu erleichtern.

[773] https://www.frontlinedefenders.org/en/statement-report/statement-targetingpalestinian-hrds-pegasus; https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/.

[774] https://www.amnesty.org/en/latest/researc h/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/.

431. Es sei darauf hingewiesen, dass die Kommission im Zusammenhang mit Berichten über den Missbrauch der Pegasus-Spähsoftware durch die NSO Group unter Verletzung der Menschenrechte mit den israelischen Behörden Kontakt aufgenommen hat. In einem Schreiben an den PEGA-Ausschuss vom 9. September 2022 antwortete die Kommission, dass sie mit den israelischen Ausfuhrbehörden die Bedenken hinsichtlich eines möglichen Missbrauchs erörtert und um Hinweise auf etwaige damit zusammenhängende eindämmende Maßnahmen ersucht habe, die die zuständigen israelischen Ausfuhrkontrollbehörden in Zukunft ergreifen könnten. Zum Zeitpunkt des Schreibens hatte die Kommission keine derartigen Hinweise von den zuständigen israelischen Ausfuhrkontrollbehörden erhalten, verfolgte aber die Absicht, während der nächsten Sitzung des Unterausschusses zu Industrie, Handel und Dienstleistungen des Assoziationsabkommens zwischen der EU und Israel auf die Frage möglicher eindämmender Maßnahmen zurückzukommen.

MAROKKO

432. Mehrere Medien berichteten vom mutmaßlichen weitreichenden Einsatz von Spähsoftware in Marokko. Mit einer Lizenz für etwa 100 000 Telefonnummern kann Marokko als einer der größten Pegasus-Kunden von NSO Group angesehen werden.[775] Marokko hat die Anschuldigungen im Zusammenhang mit dem Pegasus-Projekt als falsch zurückgewiesen. Im Dezember 2020 wurde in einem Bericht von CitizenLab aufgedeckt, dass Marokko einer der 25 Kunden von Circles ist, einer Tochtergesellschaft von NSO Group[776].

433. Die Enthüllungen zeigten auch, dass Spähsoftware angeblich innerhalb des Landes zur Überwachung genutzt wurde, um Journalisten und Aktivisten zu hacken und anschließend einzuschüchtern[777]. In einer kürzlich veröffentlichten Entschließung zur Überwachung und Inhaftierung des Enthüllungsjournalisten Omar Radi hat das Europäische Parlament die anhaltenden Schikanen der marokkanischen Regierung gegen Journalisten verurteilt und das Land aufgefordert, die „Überwachung von Journalisten, unter anderem mithilfe der Spähsoftware Pegasus des Unternehmens NSO, einzustellen“[778]. Einer der betroffenen Personen, Ignacio Cembrero, ein investigativer Journalist bei der spanischen Zeitung El Confidential, erschien am 29. November 2022 vor dem PEGA-Ausschuss. Er hatte bemerkt, dass sein Telefon gehackt worden war, nachdem Textnachrichten zwischen ihm und der spanischen Regierung in einer marokkanischen Zeitung veröffentlicht worden waren. Nach Aufforderung eines spanischen Gerichts zur Zusammenarbeit weigerten sich die israelischen Behörden, weitere Informationen zur Aufklärung des Falls zu liefern.

434. Marokko hat auch die in Frankreich im Exil lebenden marokkanischen Journalisten Hicham Mansouri und Aboubakr Jamaim[779] sowie Unterstützer der Westsahara verfolgt, namentlich den in Paris ansässigen Strafverteidiger Joseph Breham und den in

[775] https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara.
[776] https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.
[777] https://daraj.media/en/76202/.
[778] European Parliament resolution of 19 January 2023 on the situation of journalists in Morocco, notably the case of Omar Radi, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0014_EN.html.
[779] Forbidden Stories. https://forbiddenstories.org/journaliste/hicham-mansouri/, https://forbiddenstories.org/journaliste/aboubakr-jamai/.

Belgien lebenden saharauischen Menschenrechtsverteidiger El Mahjoub Maliha[780].

435. Marokko hat als Reaktion auf Anschuldigungen, es sei an der Verwendung von Pegasus in Frankreich, Spanien und Deutschland beteiligt gewesen, mehrere Gerichtsverfahren angestrengt. In Frankreich haben die marokkanischen Behörden Verleumdungsklagen gegen mehrere Medienorgane und Organisationen der Zivilgesellschaft eingereicht, darunter Le Monde, Forbidden Stories, Radio France, Mediapart, L' Humanité und Amnesty International. Am 25. März 2022 wies das Pariser Strafgericht die Klagen als unzulässig ab, woraufhin die marokkanischen Behörden Berufung gegen die Entscheidung einlegten. In Spanien reichten die marokkanischen Behörden Klage gegen den Journalisten Cembrero ein und griffen dabei auf die aus dem Mittelalter stammende Rechtsnorm des Strafgesetzbuchs zum Tatbestand der „Prahlerei" zurück. Der Fall ist noch nicht abgeschlossen und wurde als Versuch bezeichnet, Cembrero und andere davon abzuhalten, über den Einsatz der Spähsoftware in Marokko zu berichten[781].

436. Einem Nachrichtenbericht zufolge war Marokko vor dem weit verbreiteten Einsatz von Pegasus auch Kunde von mindestens drei europäischen Spähsoftware-Anbietern, namentlich der französischen Unternehmen Amesys und Vupen[782] sowie des italienischen Unternehmens Hacking Team. Vertraulichen Unterlagen zufolge war Marokko der drittgrößte Kunde des italienischen Unternehmens und zahlte über einen Zeitraum von sechs Jahren mehr als 3 Mio. EUR für den Erwerb der Software RCS von Hacking Team für seinen inländischen High Council for National Defence (CSDN) und das Directory of Territorial Surveillance (DST)[783]. Mehrere hochrangige UN-Abteilungen und -Dienste wurden mit Hilfe der Spähsoftware überwacht.

437. Marokko hat nicht nur Spähsoftware in der EU erworben, sondern auch von der Kommission technische und finanzielle Unterstützung erhalten. Nach Angaben des Spiegels hat Marokko zwei Spähsoftware-Systeme zum Ausspähen von Personen zu Grenzkontrollzwecken erhalten (Spähsoftware „XRY" des französisch-libanesischen Unternehmens MSAB und die Spähsoftware „Detective" des US-amerikanischen Unternehmens Oxygen Forensics)[784]. Darüber hinaus wurden Vertreter der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) nach Marokko entsandt, um Präsenzschulungen zur Verwendung von Spähsoftware durchzuführen und der Polizei beizubringen, wie mittels Social Hacking Informationen aus Social-Media-Profilen gewonnen werden können[785]. Im Gegensatz zu Pegasus können die genannten Spähsoftware-Anwendungen ausschließlich physisch in das Gerät eindringen und hinterlassen keine Spuren. Der Bericht skizziert mehrere Fälle, in denen Smartphones von Zielpersonen, darunter Journalisten und Aktivisten,

[780] https://www.middleeasteye.net/fr/entretien s/pegasus-espionnage-maroc-francemacron-sahara-occidental-brehamavocat-mangin-algerie.
[781] https://www.middleeastmonitor.com/20220705-morocco-files-lawsuit-against-spain-journalist-who-reported-use-of-pegasus-spyware/.
[782] https://moroccomail.fr/2022/09/21/morocco-used-hacking-team-to-spy-on-the-un/.
[783] https://privacyinternational.org/blog/1394 /facing-truth-hacking-team-leak-confirms-moroccan-government-use-spyware; https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.
[784] https://www.spiegel.de/ausland/marokkowie-die-eu-rabatsueberwachungsapparat-aufruestet-ad3f4c00e-4d39-41ba-be6c-e4f4ba65035; https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware.
[785] https://privacyinternational.org/longread/4289/revealed-eu-training-regimeteaching-neighbours-how-spy.

entwendet wurden und mit Hinweisen auf ihre mögliche Infizierung zurückkehrten. Obwohl nicht verifiziert werden kann, ob die Spähsoftware von Dritten ordnungsgemäß verwendet wurde, gab es keine Hinweise darauf, dass die Kommission die ordnungsgemäße Verwendung der gelieferten Technologien überprüft hatte. Ähnlich wie bei einer Beschwerde bei der Europäischen Ombudsstelle über die Finanzierung von Überwachungstechnologien im Rahmen des EUTFA-Programms (siehe entsprechendes Kapitel unten) hat die Kommission keine Folgenabschätzung durchgeführt, um einen möglichen Missbrauch der gelieferten Technologien zu erfassen. Die Kommission hat erklärt, dass sie Sache des Nutzers, also Marokkos, sei, die Spähsoftware verantwortungsvoll und gemäß der vertraglichen Vereinbarung einzusetzen (d. h. nur für die genannten Zwecke)[786].

ANDERE DRITTLÄNDER

438. Weltweit haben mindestens 75 Länder Spähsoftware gekauft und/oder verwendet, darunter auch repressive Regime[787]. Menschenrechtsorganisationen haben zahlreiche Vorfälle dokumentiert, bei denen Spähsoftware missbraucht wurde, um gegen Politiker, Journalisten, Rechtsanwälte, Menschenrechtsverteidiger und andere Aktivisten der Zivilgesellschaft vorzugehen, die sich für Menschenrechte, Frauenrechte und den Umweltschutz einsetzen[788].

MITTÄTERSCHAFT VON EU-MITGLIEDSTAATEN ALS KUNDEN DER NSO GROUP BEIM MISSBRAUCH VON PEGASUS IN DRITTLÄNDERN

439. Die Behörden von 14 Nicht-EU-Ländern sind höchstwahrscheinlich für viele Fälle verantwortlich, in denen die Zielpersonen identifiziert wurden und die Infizierung technisch nachgewiesen wurde. Die betreffenden Länder sind El Salvador, Mexiko, Thailand, Marokko, Indien, Ruanda, Saudi-Arabien, Bahrain, Jordanien, Kasachstan, Togo, die VAE, Israel und Aserbaidschan[789].

440. Im Rahmen des Pegasus-Projekts, einer Zusammenarbeit von mehr als 80 Journalisten von 17 Medienorganen, wurde dokumentiert, wie Pegasus von repressiven Regierungen eingesetzt wird, um Journalisten zum Schweigen zu bringen, Aktivisten anzugreifen und abweichende Meinungen zu unterdrücken. Recherchen des Pegasus-Projekts haben ergeben, dass Familienangehörige des saudi-arabischen Journalisten Jamal Khashoggi vor und nach seiner Ermordung in Istanbul am 2. Oktober 2018 von saudi-arabischen Akteuren mit der Pegasus-Spähsoftware ins Visier genommen wurden, auch wenn die NSO Group dies wiederholt von sich gewiesen hat. Das Security Lab von Amnesty International hat festgestellt, dass die Pegasus-Spähsoftware nur vier Tage nach der Ermordung Jamal Khashoggis erfolgreich auf dem Telefon seiner Verlobten, Hatice Cengiz, installiert wurde. Auch seine Frau Hanan Elatr wurde zwischen September 2017 und April 2018 wiederholt mit der Spähsoftware ins Visier genommen, ebenso sein Sohn Abdullah, der zusammen mit anderen Familienangehörigen in Saudi-Arabien

[786] https://disclose.ngo/en/article/how-theeu-supplied-morocco-with-phonehacking-spyware.
[787] Carnegie Endowment for International Peace, ‘Global Inventory of Commercial Spyware & Digital Forensics’, 11 January 2023, https://carnegieendowment.org/programs/democracy/commercialspyware.
[788] Forensic Architecture, Amnesty International and The Citizen Lab, ‘Digital Violence’, https://www.digitalviolence.org/#/.
[789] https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.

und den Vereinigten Arabischen Emiraten ebenfalls als Ziel ausgewählt wurde[790].

441. Zudem hat das Pegasus-Projekt festgestellt, dass Journalisten häufig Ziel der Pegasus-Spähsoftware waren. In Mexiko wurde das Telefon von Cecilio Pineda nur Wochen vor seiner Tötung im Jahr 2017 für eine Überwachung ausgewählt. Pegasus wurde auch in Aserbaidschan eingesetzt, einem Land, in dem es nur noch wenige unabhängige Medienorgane gibt. Den Ermittlungen zufolge wurden mehr als 40 aserbaidschanische Journalisten als potenzielle Ziele ausgewählt. Das Security Lab von Amnesty International fand heraus, dass das Telefon von Sevinc Vaqifqizi, einem freiberuflichen Journalisten des unabhängigen Medienunternehmens Meydan TV, über einen Zeitraum von zwei Jahren hinweg bis Mai 2021 infiziert war. In Indien wurden zwischen 2017 und 2021 mindestens 40 Journalisten von fast allen großen Medienorganen des Landes als potenzielle Ziele ausgewählt. Forensische Tests ergaben, dass die Telefone von Siddharth Varadarajan und MK Venu, den Mitbegründern des unabhängigen Online-Medienorgans The Wire, noch im Juni 2021 mit der Pegasus-Spähsoftware infiziert wurden[791].

442. Menschenrechtsverteidiger werden nach wie vor häufig zu Zielen ernannt, unter anderem von den Behörden der folgenden Länder: Mexiko, El Salvador, Marokko, Ruanda, Israel, Jordanien, Saudi-Arabien, Bahrain, den Vereinigten Arabischen Emiraten, Indien, Kasachstan, Indonesien und Belarus[792]. 2021 veröffentlichte Frontline Defenders einen Bericht, in dem die gezielte Überwachung von Menschenrechtsverteidigern in Ländern wie u. a. Indien dokumentiert wurde. Im Juni 2018 wurden 16 Menschenrechtsverteidiger im Rahmen der Antiterrorgesetzgebung aufgrund der inzwischen als Bhima-Koregaon-Fall bekannten Vorfälle inhaftiert, die mit der Gewalt in Bhima Koregaon in Zusammenhang stehen. Einer der Menschenrechtsverteidiger, der 84-jährige Jesuitenpriester Stan Swamy, verstarb im Juli 2021 in Haft[793]. Eine digitale forensische Untersuchung ergab, dass die sogenannten Beweismittel, auf die sich die Anklage gegen die Gruppe stützte, mithilfe der Spionagesoftware Pegasus auf Geräten der Menschenrechtsverteidiger Rona Wilson und Surendra Gadling platziert worden waren, und dass es keine Beweise dafür gab, dass die Menschenrechtsverteidiger miteinander interagiert hatten[794].

II. Die Spähsoftware-Branche

443. Die Europäische Union ist ein attraktiver Ort für den Handel mit Überwachungstechnologien und -dienstleistungen, einschließlich Spyware-Tools. Zum

---

[790] Amnesty International, „Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally", 19. Juli 2021, https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/.

[791] Amnesty International, „Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally", 19. Juli 2021, https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/.

[792] https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/; https://www.amnesty.org/en/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/.

[793] Frontline Defenders (2. Dezember 2021): Action needed to address targeted surveillance of human rights defenders https://www.frontlinedefenders.org/en/stat ement-report/action-needed-addresstargeted-surveillance-human-rightsdefenders.

[794] The Wire, Rona Wilson's iPhone Infected With Pegasus Spyware, Says New Forensic Report, 17. Dezember 2021, https://thewire.in/rights/rona-wilsonpegasus-iphone-arsenal.

einen sind die Regierungen der Mitgliedstaaten potenzielle Kunden. Zum anderen dient die Wahrnehmung als „EU-reguliert“ als Maßstab, der für den globalen Markt nützlich ist. Der EU-Binnenmarkt bietet Freizügigkeit und vorteilhafte nationale Steuerregelungen. Vorschriften in Bezug auf die Beschaffung können mit Hinweis auf die nationale Sicherheit umgangen werden, und die Regierungen können auf Vertreter oder Mittelsmänner zurückgreifen, sodass der Kauf von Spyware durch öffentliche Stellen sehr schwer festzustellen und zu beweisen ist. Die EU verfügt über strenge Ausfuhrvorschriften, doch in jüngster Zeit ist ein Trend dahingehend zu beobachten, dass die Mitgliedstaaten diese Vorschriften umgehen und versuchen, sich durch unangemessene Umsetzung auf nationaler Ebene einen Wettbewerbsvorteil zu verschaffen. Außerdem war die Kontrolle durch die Kommission oft unzureichend. Tatsächlich verlegten mehrere Unternehmen ihre Exportabteilungen immer dann nach Europa, wenn die Regelungen für Ausfuhrgenehmigungen in Israel verschärft wurden, insbesondere nach Zypern[795][796]. Darüber hinaus haben mehrere Personen aus der Spähsoftware-Branche eine EU-Staatsbürgerschaft erlangt, um frei innerhalb der EU und aus der EU heraus agieren zu können.

444. Wie der Leiter von Amnesty Tech, Claudio Guarniery, vor dem PEGA-Ausschuss aussagte, waren europäische Unternehmen wie das deutsche Unternehmen FinFisher und das italienische Unternehmen Hacking Team die Vorreiter der Söldner der Spähsoftware-Industrie. Die ersten Berichte über die Rolle dieser Unternehmen bei der Überwachung von Journalisten und der Unterdrückung abweichender Meinungen wurden vor über zehn Jahren bekannt, als mit dem Aufkommen der Protestbewegungen, die als „Arabischer Frühling“ bekannt sind, Verträge mit diesen Unternehmen aus Büros der Geheimpolizei auftauchten[797].

445. Die Branche der Spähsoftware ist ein undurchdringliches Labyrinth von Personen, Standorten, Verbindungen, Eigentumsstrukturen, Briefkastenfirmen, sich ständig ändernden Firmennamen, Geldströmen, von der Regierung beauftragten Akteuren (Proxies) und Mittelsleuten, Tycoons und Regierungen.

446. In vielen Fällen scheint die Bezeichnung „Söldner-Spyware“ angebracht. Wie die Zahl der unrechtmäßig ins Visier genommenen Personen zeigt, halten viele Unternehmen ethische Standards nicht ein und verkaufen oft an Diktaturen und wohlhabende nichtstaatliche Akteure, was sie auch nach den Enthüllungen des Pegasus-Projekts weiterhin tun. Nach den Enthüllungen des Pegasus-Projekts kündigte Cellebrite 2021 an, man wolle den Verkauf an die russische Regierung stoppen, wenn sich herausstellen sollte, dass Spähsoftware gegen putinkritische Aktivisten eingesetzt wird. Im Oktober 2022 gab es jedoch Hinweise darauf, dass Cellebrite weiterhin von den russischen Behörden genutzt wurde[798]. Der Markt ist lukrativ und vielschichtig. Trotzdem schaffen es viele Spähsoftware-Unternehmen, ihre Produkte an demokratische Regierungen in den USA und der EU zu verkaufen, was ihnen den

[795] Makarios Drousiotis, ‘State Mafia’, 2022, Kapitel 6.
[796] Haaretz. ‘Cyprus, Cyberspies and the Dark Side of Israeli Intel’.
[797] PEGA-Anhörung vom 30. August 2022 zu den Auswirkungen von Spyware auf EU-Bürger, https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/.
[798] https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000.

Anschein von Seriosität verleiht. Trotz der Beteuerungen, dass die Nutzung von Spähsoftware vollkommen rechtmäßig und notwendig sei, zögern die Regierungen jedoch, zuzugeben, dass sie Spähsoftware besitzen. Manchmal greifen sie für den Kauf von Spyware auf Vertreter, Mittelsmänner oder Vermittler zurück, um keine Spuren zu hinterlassen. Die größte jährliche Veranstaltung der Branche ist die Messe „ISS World“, auch bekannt als „The Wiretappers‘ Ball“. Die europäische Version findet jedes Jahr in Prag statt. Zwischen den Ausstellern bei der ISS World und Ausstellern auf Messen der Waffenindustrie gibt es erhebliche Überschneidungen.

447. Neben den „offiziellen Kanälen“ gibt es auch einen Schwarzmarkt für diese Produkte. Obwohl viele Anbieter behaupten, Verkäufe erfolgten ausschließlich an Regierungen, scheinen sie zu versuchen, ebenfalls Geschäfte mit nichtstaatlichen Akteuren zu tätigen. Es ist äußerst schwierig, stichhaltige Beweise zu finden, da dieser Handel kaum Spuren hinterlässt. Der griechischen Zeitung Documento liegen nach eigener Aussage Beweise dafür vor, dass die Software auf dem Schwarzmarkt – für bis zu 50 Mio. US-Dollar – nicht nur an Regierungen und Anti-Terror-Behörden, sondern auch an Privatpersonen verkauft wird[799]. Eine weitere griechische Zeitung, To Vima, berichtete, dass Predator an 34 Kunden aus Griechenland verkauft wurde[800]. Durchgesickerte Dokumente zeigen, dass eine raubkopierte Version des Produkts, die offiziell nur an Regierungen verkauft wurde, zu einem Preis von 8 Mio. USD erhältlich war, ein Betrag, der die Schulung der Beauftragten, die das Programm nutzen werden, den technischen 24-Stunden-Support und die Überwachung der Social-Media-Konten der Zielperson umfasste[801].

448. Die Branche bietet ein breites Spektrum an Überwachungs- und nachrichtendienstlichen Produkten und entsprechenden Diensten an, nicht nur Spähsoftware als solche. Spähsoftware ist nur ein Werkzeug von vielen, die von Hack-for-Hire-Unternehmen angeboten werden.

Schwachstellen

449. Ohne Schwachstellen in der Software wäre es unmöglich, Spähsoftware zu installieren und einzusetzen. Um die Verwendung von Spyware zu regulieren, müssen deshalb die Aufdeckung, die Offenlegung und die Ausnutzung von Schwachstellen ebenfalls reguliert werden[802]. Trotz der Stärkung der Abwehr digitaler Systeme, die durch die NIS2-Richtlinie und das vorgeschlagene Cyberresilienzgesetz vorgeschrieben und gefördert wurde, ist es nahezu unmöglich, Systeme ohne Schwachstellen zu entwickeln.

450. Daher müssen Schwachstellen möglichst rasch offengelegt und behoben werden. Das geltende Unionsrecht fördert jedoch das Gegenteil einer Offenlegung. Gemäß der Richtlinie zur Bekämpfung der Cyberkriminalität und der Urheberrechtsrichtlinie können Wissenschaftler aus dem Bereich Informationssicherheit zivil- und strafrechtlich haftbar gemacht werden, wenn sie Forschungen zu Schwachstellen

[799] Documento, ‘Documento’s “Predator” revelations on Euractiv – Europol’s intervention calls for Dutch MEP’.
[800] To Vima, Interceptions ‘Spy software has 34 customers’.
[801] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/.
[802] Ot van Daalen, Intervention im PEGA-Ausschuss, 27. Oktober 2022;

EDRi Paper: ‘Breaking encryption will doom our freedoms and rights’, https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-Encryption.pdf;
https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu.

betreiben und ihre Ergebnisse weitergeben. Darüber hinaus sind Wissenschaftler nicht verpflichtet, Erkenntnisse über Schwachstellen weiterzugeben. Wissenschaftler könnten sich daher dafür entscheiden, das Wissen über Schwachstellen gegen hohe Vergütungen an private Vermittler zu verkaufen.

451. Diese Praxis hat zu einem lebhaften, lukrativen Handel mit Schwachstellen geführt. Es sind jedoch nicht nur Makler für Zero-Day-Schwachstellen, die nach Schwachstellen suchen: Auch Sicherheits- und Strafverfolgungsbehörden sammeln Kenntnisse über Schwachstellen, einige davon durch ihren eigenen Experten aufgedeckt, einige über Mittler erworben. Wenn Schwachstellen nicht gemeldet werden, werden sie nicht behoben, so dass die IT-Systeme geschwächt und die Nutzer ungeschützt sind. Auf diese Weise kann weiterhin Spähsoftware eingesetzt werden.

Telekommunikationsnetze

452. Telekommunikationsanbieter spielen eine wichtige Rolle bei der legalen und illegalen Spionage. Wir leben in einem modernen Zeitalter von KI, Big Data und Quantencomputing, aber gleichzeitig nutzen wir ein internationales Telekommunikationsprotokoll namens Signalling System No 7 (SS7) und verlassen uns stark darauf. Dieses Protokoll wurde 1975 entwickelt und wird auch heute noch verwendet. Mit diesem System wird gesteuert, wie Anrufe geroutet und abgerechnet werden und ermöglicht fortschrittliche Anruf-Features und Kurznachrichtendienste (SMS)[803]. Über das SS7-Netzwerk ist es möglich, Telefonanrufe und SMS-Nachrichten abzufangen, Geolokalisierungen zu identifizieren und ein Ziel mit Spähsoftware wie Pegasus oder Predator zu infizieren[804].

453. Das Risiko, dass Telekommunikationsanbieter den Zugang zu diesen Netzen missbrauchen, ist hoch. Es gibt mehrere dokumentierte Fälle von Missbrauch, bei denen Zugangspunkte („Global Titles“) an Unternehmen verleast wurden, die die Kommunikation von Zielpersonen mit Hilfe von Man-in-the-Middle-Angriffen überwachten und abfingen. Sie erhoben auch Geolokalisierungsdaten und Metadaten für ihre eigenen wirtschaftlichen Zwecke. Ein „globaler Titel“ ist eine Adresse, die für das Routing von Nachrichten innerhalb von SS7 verwendet wird. Ein Global Title ist mit einer IP-Adresse insofern vergleichbar, als er sich auf eine Adresse innerhalb des Telekommunikationssystems bezieht[805]. Laut einem Whistleblower war genau deshalb der Zugang zum SS7-System in den Vereinigten Staaten von Amerika für die NSO Group auch so interessant, dass sie versuchte, sich den Zugang zu erkaufen[806]. Telekommunikationsanbieter erhalten absichtlich niedrige Industriestandards aufrecht, um den lokalen Strafvollzugsbehörden einen leichteren Zugang zu ermöglichen.

Die NSO Group

454. Die Spähsoftware „Pegasus“ wird von der NSO Group produziert. Die NSO Group

---

[803] https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7 was first adopted as, up to and including 5G.
[804] https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/.
[805] https://www.gms-worldwide.com/glossary/global-title/.
[806] https://www.theguardian.com/news/2022/feb/01/nso-offered-us-mobile-security-firm-bags-of-cash-whistleblower-claims.

wurde 2010 von Shalev Hulio, Omri Lavie und Niv Karmi gegründet, um Technologien zu entwickeln, die lizenzierten Regierungsagenturen und Strafverfolgungsbehörden dabei helfen, Terrorismus und Kriminalität aufzudecken und zu verhindern[807]. Die Pegasus-Spähsoftware ist das bekannteste Produkt der NSO Group. Sie wurde 2011 auf den Weltmarkt gebracht.[808][809]

455. Seit ihrer Gründung im Jahr 2010 verfügt die NSO Group in Israel, im Vereinigten Königreich, in Luxemburg, auf den Kaimaninseln, in Zypern, in den USA, den Niederlanden, in Bulgarien und auf den Britischen Jungferninseln über Unternehmenspräsenzen. Es fehlen nach wie vor viele Informationen über die Rolle der einzelnen Gesellschaften, und einige wurden bereits liquidiert. Die NSO Group hat jedoch in ihrem Bericht über Transparenz und Verantwortung aus dem Jahr 2021 erklärt, dass Bulgarien und Zypern Exportknotenpunkte sind[810]. Nach Angaben von Amnesty International waren die (am 22. Dezember 2016 liquidierten) niederländischen Gesellschaften im Bereich Finanzholding tätig, und Q Cyber Technologies mit Sitz in Luxemburg war als Vertriebsgesellschaft tätig, die für die Ausstellung von Rechnungen, die Unterzeichnung von Verträgen und die Entgegennahme von Zahlungen von Kunden zuständig war. Darüber hinaus könnte Westbridge Technologies mit Sitz in den USA für die US-Verkäufe des Unternehmens zuständig gewesen sein[811].

456. Im Jahr 2020 erwirtschaftete NSO Berichten zufolge Einnahmen in Höhe von 243 Mio. US-Dollar[812]. Nach den Enthüllungen im Rahmen des Pegasus-Projekts sah sich das Unternehmen jedoch mit verschiedenen Problemen konfrontiert, namentlich führten die Klagen von Apple[813] und Meta[814] gegen das Unternehmen, der Umstand, dass das US-Handelsministerium NSO auf eine schwarze Liste setzte, die Verschärfung der Ausfuhrregelung Israels, kritische Untersuchungen in mehreren Ländern sowie interne Spannungen innerhalb des Private-Equity-Fonds hinter der NSO Group zu einem erheblichen Rückgang der Gewinne. Berichten zufolge erreichten die Schulden der NSO Group zu einem Zeitpunkt sogar das 6,5fache der gewöhnlichen Jahreseinnahmen des Unternehmens[815].

457. Der PEGA-Ausschuss hatte zwei Sitzungen mit der NSO Group, von denen eine in Brüssel und eine in Israel stattfand. Die Pegasus-Spähsoftware wurde ursprünglich an 22 Endnutzer in 14 Mitgliedstaaten der EU verkauft, wobei von Israel erteilte Vermarktungs- und Ausfuhrlizenzen genutzt wurden. Verträge mit Endnutzern in zwei Mitgliedstaaten wurden anschließend gekündigt[816]. Es wurde weder bestätigt, welche Mitgliedstaaten in der Liste der 14 Länder erscheinen, noch, welche beiden Länder gestrichen wurden. Es ist jedoch anzunehmen, dass es sich um Polen und Ungarn

[807] NSO Group. „About us“.
[808] The New York Times „The Battle for the World’s Most Powerful Cyberweapon“.
[809] Shalev Hulio, „NSO Never Engaged in Illegal Mass Surveillance“, The Wall Street Journal, 24. Februar 2022.
[810] NSO Group, „Transparency and Responsibility Report 2021“.
[811] Amnesty International „Operating from the shadows – inside NSO Group’s corporate structure“.
[812] Haaretz, „NSO Is Having a Bad Year - and It’s Showing“.
[813] Apple „Apple sues NSO Group to curb the abuse of state-sponsored spyware“.
[814] Bloomberg Law, ‘NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware“.
[815] Bloomberg, „Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop“.
[816] Antworten der NSO Group an das PEGA-Sekretariat im Anschluss an eine Anhörung, 20. Juli 2022.

handelt.

UNTERNEHMENSSTRUKTUR, TRANSPARENZ UND SORGFALTSPFLICHT

458. Am 25. Januar 2010 gründete die NSO Group ihr erstes Unternehmen in Israel. Dieses Unternehmen wurde unter dem Namen „NSO Group Technologies Limited“ registriert. NSO Group ist sowohl der Name des ersten registrierten Unternehmens als auch der Überbegriff für verschiedene in anderen Ländern gegründete Unternehmen. Das zuerst gegründete Unternehmen ist Eigentümer der Marke „NSO Group“.[817]

459. Im März 2014 erwarb der Private-Equity-Fonds Francisco Partners 70 % an der NSO Group. Unter Francisco Partners weitete das Unternehmen seine Gesellschaften auf verschiedene Länder aus, darunter Zypern, Bulgarien, die Vereinigten Staaten von Amerika, die Niederlande und Luxemburg. In den Jahren 2014 bis 2019, in denen Francisco Partner Anteile an der NSO Group hielt, ließ der Fonds den Verkauf der Produkte der NSO Group durch das Business Ethics Committee (BEC) systematisch überprüfen. Nach Angaben von Francisco Partners hat das BEC Verkäufe in Höhe zweistelliger Millionen-Beträge in US-Dollar verweigert, die nach den gesetzlichen Anforderungen genehmigt worden wären[818].

460. Amnesty International, „Operating from the shadows - inside NSO Group’s corporate structure“. Mit diesem Management-Buy-out änderten sich die Governance-Standards, und an die Stelle des BEC trat das Governance, Risk and Compliance Committee (Ausschuss für Governance, Risiken und Compliance, GRCC), das die Überprüfung der Menschenrechtsbilanz potenzieller Kunden übernahm[819].

461. Im Einklang mit der Endverbleibserklärung nach der Verschärfung der israelischen Ausfuhrregelung führte die NSO Group eine Menschenrechtsstrategie und ein Verfahren zur Sorgfaltspflicht im Bereich der Menschenrechte ein. Wie im Bericht über Transparenz und Verantwortung der NSO Group aus dem Jahr 2021 dargelegt, schreibt die NSO Group vor, dass alle Kundenvereinbarungen Klauseln zur Einhaltung der Menschenrechte und Klauseln über die Aussetzung oder Beendigung der Verwendung der Produkte der NSO Group im Falle von missbräuchlicher Verwendung im Zusammenhang mit den Menschenrechten enthalten. In einer schriftlichen an den PEGA-Ausschuss gerichteten Stellungnahme bestätigte die NSO Group, dass sie Verträge mit Mitgliedstaaten der EU[820] gekündigt habe, die mutmaßlich gegen die Menschenrechtsklauseln verstoßen hatten. Die NSO Group hat nicht dargelegt, ob sie eine Prüfung der Audit-Logs vorgenommen hat und ob die betreffenden Kunden einer Prüfung zugestimmt hatten. Es ist daher nicht bekannt, ob noch Beweise für die missbräuchliche Verwendung vorliegen, ob die NSO Group diese Beweise auf irgendeine Weise sichern kann und ob die israelischen Behörden über Beweise verfügen.

462. Laut Amnesty International fehlt im Transparenzbericht der NSO Group eine angemessene Wiedergutmachungsstrategie für Opfer rechtswidriger Überwachung, und

[817] Amnesty International, „Operating from the shadows - inside NSO Group’s corporate structure“.
[818] Amnesty International, „Operating from the shadows - inside NSO Group’s corporate structure“.
[819] Anhörung der NSO Group durch den PEGA-Ausschuss, 21. Juni 2022.
[820] Anhörung der NSO Group durch den PEGA-Ausschuss, 21. Juni 2022.

es fehlen Informationen über die gegen die NSO Group laufenden Gerichtsverfahren[821]. NSO-Spähsoftware wird entgegen der Menschenrechtsstrategie und des Verfahrens zur Sorgfaltspflicht im Bereich der Menschenrechte von NSO nach wie vor auf Geräten von Journalisten und Kritikern autoritärer Regime entdeckt[822].

AUSFUHRKONTROLLEN

463. Da Pegasus-Spähsoftware als Technologie mit doppeltem Verwendungszweck gilt, wird dafür eine Ausfuhrgenehmigung benötigt. Die Unternehmen der NSO Group erhalten ihre Ausfuhrgenehmigungen in Israel, Bulgarien und Zypern[823]. Die NSO Group hat dies bestätigt, bestreitet aber, dass die Pegasus-Spähsoftware aus Zypern und Bulgarien ausgeführt wird[824]. Die zyprische Regierung sowie die bulgarische Regierung bestreiten, überhaupt Ausfuhrgenehmigungen für NSO-Unternehmen erteilt zu haben. Andere Quellen haben dies in Frage gestellt und erklärt, dass sich Tochtergesellschaften der NSO Group in den nationalen Unternehmensregistern häufig unter anderem Namen verstecken. Eine der Tochtergesellschaften von NSO in Zypern, die unter dem Namen „Circles“ firmierte, schloss im Jahr 2020 jedoch ihre Büros[825]. Lizenzen werden auch von den israelischen Behörden erteilt[826]. Israel ist nicht Teil des Wassenaar-Abkommens, erklärt aber, einige Elemente daraus in sein nationales Gesetz über die Kontrolle von Ausfuhren im Verteidigungsbereich (5766) von 2007 übernommen zu haben[827]. Die Agentur für die Kontrolle von Ausfuhren im Verteidigungsbereich des Verteidigungsministeriums ist für die Erteilung von Vermarktungs- und Ausfuhrgenehmigungen zuständig[828]. Nach den Enthüllungen des Pegasus-Projekts und dem Blacklisting von NSO wurde die Liste der in Betracht kommenden Länder von 102 auf 37 gekürzt, die alle eine Endverbleibserklärung unterzeichnen müssen[829]. In den Verfahren zur Erfüllung der Sorgfaltspflicht geht Israel automatisch davon aus, dass alle EU-Mitgliedstaaten die EU-Normen erfüllen, und führt deshalb keine zusätzlichen Überprüfungen einzelner Länder durch. Die Entscheidung, die Verträge mit zwei EU-Mitgliedstaaten zu kündigen, scheint jedoch darauf hinzudeuten, dass die EU im Hinblick auf die Sorgfaltspflicht nicht mehr als eine zentrale Stelle betrachtet wird.

GERICHTSVERFAHREN, BLACKLISTING UND INVESTORENKONFLIKTE AUFGRUND UNETHISCHEN VERHALTENS

464. Im Juli 2021 begann sich ein Konflikt zwischen den drei Gründern von Novalpina Capital auf die Geschäftstätigkeit der NSO Group auszuwirken, was schließlich dazu führte, dass die Investoren entschieden, der Private-Equity-Gesellschaft die Kontrolle zu

[821] Amnesty International, „NSO Group's new transparency report is 'another missed opportunity'“, Presseerklärung, 1. Juli 2021.
[822] The New York Times, „U.S. Blacklists Israeli Firm NSO Group Over Spyware“.
[823] Amnesty International, „Operating from the shadows – inside NSO Group’s corporate structure“, S. 62.
[824] Amnesty International, „Operating from the shadows – inside NSO Group’s corporate structure“.
[825] VICE, „NSO Group Closes Cyprus Office of Spy Firm“.
[826] Amnesty International, „Operating from the shadows – inside NSO Group’s corporate structure“.
[827] Wissenschaftlicher Dienst des Europäischen Parlaments, „Europe’s PegasusGate – countering spyware abuse“.
[828] Amnesty International, „Novalpina Capital’s reply to NGO coalition letter (15 April 2019) and Citizen Lab letter (6 March 2019)“.
[829] Wissenschaftlicher Dienst des Europäischen Parlaments, „Europe’s PegasusGate – countering spyware abuse“.

entziehen[830]. Am 27. August 2021 übernahm das US-Beratungsunternehmen Berkeley Research Group (BRG) den Private-Equity-Fonds und leitete kritische Untersuchungen in Bezug auf die Gesetzmäßigkeit der Aktivitäten der NSO Group und ihre Erfüllung der US-Blacklisting-Vorschriften ein. Die Untersuchungen der BRG vom Mai 2022 wurden vom Führungsteam der NSO Group behindert[831]. Ein leitender BRG-Mitarbeiter erklärte, die Zusammenarbeit mit der NSO Group sei aufgrund des Drucks der NSO Group, weiter in Länder mit umstrittener Menschenrechtslage zu verkaufen, „so gut wie nicht vorhanden“[832]. Am 25. April 2022 reichten zwei der ehemaligen Komplementäre von Novalpina bei einem Luxemburger Gericht eine Klage gegen BRG ein, in der sie die Wiedereinsetzung von Novalpina Capital als Komplementär und die Rücknahme aller von BRG getroffenen Entscheidungen forderten[833]. Das Luxemburger Gericht wird diese Forderungen ab, und BRG bleibt für den Fonds, der die NSO Group kontrolliert, verantwortlich[834].

465. Zusätzlich zu den Auswirkungen auf die Eigentumsverhältnisse setzte das US-Handelsministerium die NSO Group am 3. November 2021 mit der Begründung auf eine schwarze Liste, ihre Tätigkeiten seien nicht mit der US-Außenpolitik und nationalen Sicherheitsbelangen vereinbar. Die US-Regierung untersagt die Ausfuhr von Technologien an die NSO Group und ihre Tochtergesellschaften, was *de facto* bedeutet, dass US-amerikanische Unternehmen nicht mit der NSO Group zusammenarbeiten können[835].

466. Als Reaktion auf die Aufnahme auf die schwarze Liste in den Vereinigten Staaten von Amerika hat Credit Suisse als einer der Gläubiger der NSO Group das Unternehmen angeblich dazu veranlasst, seine Verkäufe der Spähsoftware „Pegasus“ an neue Kunden fortzusetzen. In einem Schreiben von Willkie Farr & Gallagher an die Berkeley Research Group (BRG) erklärten mehrere Gläubiger, sie hätten Bedenken dahingehend, dass die BRG die NSO Group daran hindere, Neukunden zu ermitteln und zu gewinnen. Obwohl dies in dem Schreiben nicht ausdrücklich angegeben wurde, gaben zwei Experten auf dem Gebiet an, dass einer der Gläubiger Credit Suisse sei. Die BRG antwortete den Kreditgebern, sie sei zutiefst besorgt darüber, wie nachdrücklich darauf hingewirkt werde, dass die NSO Group ihre Verkäufe fortsetze[836].

467. Nur wenige Tage nach der Aufnahme von NSO in die schwarze Liste durch die Vereinigten Staaten von Amerika ließ das Berufungsgericht der Vereinigten Staaten die Klage von Meta gegen NSO zu. Unmittelbar danach reichte Apple eine Klage gegen NSO bei einem Bundesgericht ein[837]. Im Juni 2022 wies ein US-Bundesbezirksgericht den Antrag der NSO Group auf Immunität in der Apple-Klage zurück[838]. Zum Zeitpunkt der Erstellung dieses Berichts ist die Klage von Apple gegen die NSO Group

---

[830] Financial Times, „Private equity owner of spyware group NSO stripped of control of €1bn fund“.
[831] Financial Times, „NSO Group keeping owners ‚in the dark‘, manager says“.
[832] The New Yorker, „How democracies spy on their citizens“.
[833] Schreiben an Jeroen Lenaers und seine stellvertretenden Vorsitzenden.
[834] Luxembourg Times, „Top five stories you may have missed“.
[835] The New York Times, „U.S. Blacklists Israeli Firm NSO Group Over Spyware“.
[836] Financial Times, „Credit Suisse pushed for spyware sales at NSO despite US blacklisting“.
[837] The New York Times, „Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones“.
[838] https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/35/.

noch anhängig.

468. Trotz der Aufnahme von NSO auf die schwarze Liste der Vereinigten Staaten von Amerika hat die Biden-Administration im Oktober 2022 angeblich den ehemaligen NSO-Berater Jeremy Bash für die Mitgliedschaft in einem nachrichtendienstlichen Beratungsausschuss ernannt. Bash war für Beacon Global Strategies tätig und wurde angeblich angeworben, um über Francisco Partners als Berater für die NSO Group zu fungieren. Nach Angaben des Guardian war er eines der acht Mitglieder des Ausschusses für Unternehmensethik der NSO Group und hatte somit angeblich ein Stimmrecht in Bezug auf geplante Verkäufe durch die NSO Group. Beacon Global Strategies beendete die Zusammenarbeit mit NSO infolge der angestrebten Verkäufe an Saudi-Arabien[839].

469. Die NSO Group hatte zudem Personalabgänge zu verzeichnen. Seit dem Mord an Jamal Khashoggi und der wachsenden Besorgnis um die Rolle von Pegasus in diesem Fall haben viele Mitarbeitende die NSO Group verlassen Im selben Monat trat Mitbegründer Shalev Hulio als Geschäftsführer der NSO Group zurück und wurde durch Yaron Shohat ersetzt[840]. Die NSO Group änderte ihre Politik und konzentriert sich jetzt nur noch auf Mitglieder der NATO[841]. Im März 2023 wurde berichtet, dass NSO-Anteile an die Investmentfirma Dufresne Holding des Mitbegründers Omri Lavie übertragen wurden[842].

470. Der Druck auf die NSO Group hat zu einer Nachfrage nach anderen Unternehmen für Spähsoftware geführt. Die Financial Times berichtete am 31. März 2023, dass die indische Regierung angeblich nach einer Gelegenheit suchte, alternative kommerzielle Spähsoftware mit ähnlichen Funktionalitäten wie die jetzt umstrittene Pegasus-Spähsoftware zu kaufen, und dass sie auch die Predator-Spähsoftware von Intellexa in Betracht zog[843].

471. Im Oktober 2022 gründeten Shalev Hulio und der ehemalige österreichische Bundeskanzler Sebastian Kurz eine neue Cybersicherheitsfirma namens „Dream Security“. Kurz war nach einem Korruptionsskandal im Oktober 2021 vom Amt des Bundeskanzlers zurückgetreten und nahm zwei Monate später eine Tätigkeit für die Investmentfirma von Peter Thiel auf. Das Unternehmen wird Lösungen im Bereich Cybervorfälle entwickeln, deren Schwerpunkt auf künstlicher Intelligenz liegt, und es wird seine Verkäufe auf den europäischen Markt konzentrieren[844]. Die Zusammenarbeit zwischen Kurz und Hulio stellt eine indirekte, aber alarmierende Verbindung zwischen der Industrie für Spähsoftware sowie Peter Thiel und seiner Firma Palantir dar.

472. Dream Security hat 20 Mio. USD von mehreren Investoren erhalten, darunter Adi Shalev, der auch in NSO investiert hatte. Weitere Investoren sind Yevgeny Dibrov[845],

---

[839] The Guardian, „Biden intelligence advisor previously vetted deals for Israeli NSO Group“.
[840] The Washington Post, „CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup“; Calcalist, „After cutbacks and CEO departure, what’s next for the controversial NSO?“.
[841] The Guardian, „CEO of Israeli Pegasus spyware firm NSO to step down“.
[842] The Guardian „NSO Group co-founder emerges as new majority owner“.
[843] https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9.
[844] Organised Crime and Corruption Reporting Project, „Former Austrian Chancellor and ex-NSO Chief Start Cybersecurity Firm“; The Times, „Former NSO CEO and ex-Austrian Chancellor found startup“.
[845] The Times, „Former NSO CEO and ex-Austrian Chancellor found startup“.

der die neue russische Stimme in dem wie er es nennt „russisch-israelischen Tech-Ökosystem“ vertrete[846]. Dies zeigt, dass trotz der Turbulenzen und wirtschaftlichen Herausforderungen, mit denen die NSO Group konfrontiert ist, die gleichen Namen weiterhin neue Spähsoftware-Unternehmen innerhalb und außerhalb der EU gründen.

BLACK CUBE

473. Bei der Firma Black Cube handelt es sich um einen privaten israelischen Nachrichtendienst, für den ehemalige Mitarbeiter des israelischen Militärs und der israelischen Geheimdienste tätig sind[847]. Auf seiner eigenen Website bezeichnet sich das Unternehmen als kreativen Nachrichtendienst, der maßgeschneiderte Lösungen für komplexe geschäftliche und rechtliche Herausforderungen findet.[848] Black Cube war in eine Reihe von öffentlichen Kontroversen um Hackerangriffe verwickelt, unter anderem in Ländern wie den USA und Rumänien[849]. Insbesondere räumte die Black Cube-Führung ein, die frühere leitende Staatsanwältin der rumänischen nationalen Antikorruptionsdirektion, Laura Kovesi, ausspioniert zu haben[850]. Laura Kovesi ist derzeit die erste Europäische Generalstaatsanwältin und leitet die Europäische Staatsanwaltschaft (EUStA). Angeblich war der frühere rumänische Geheimagent Daniel Dragomir derjenige, der Black Cube mit diesem Job beauftragt hat[851].

474. Außerdem wurde aufgedeckt, dass Black Cube mit der NSO Group und Pegasus-Spähsoftware in Verbindung steht. Nach dem großen öffentlichen Druck in Bezug auf die Beauftragung von Black Cube durch NSO, um ihre Gegner ins Visier zu nehmen, räumte der ehemalige CEO von NSO Shalev Hulio ein, Black Cube in mindestens einem Fall in Zypern beauftragt zu haben.

475. Black Cube war während der Wahlen 2018 in Ungarn aktiv, spionierte verschiedene nichtstaatliche Organisationen und Personen aus, die in irgendeiner Weise mit George Soros in Verbindung standen, und erstattete Viktor Orbán Bericht, damit dieser ihre Aktivitäten in einer Verleumdungskampagne ausschlachten konnte[852]. Die sich aus der Überwachung dieser Personen und NGO ergebenden Informationen erschienen nicht nur in den staatlich kontrollierten ungarischen Medien, sondern auch in der Jerusalem Post[853].

INTELLEXA ALLIANCE

476. Intellexa wurde 2019 von Tal Dilian in Zypern gegründet. Dilian bekleidete verschiedene Führungspositionen bei den israelischen Streitkräften, bevor er eine

---

[846] Calcalist, „From Russia, With Coding Skills“.
[847] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7. Oktober 2019.
[848] https://www.blackcube.com/.
[849] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. April 2022.
[850] Balkan Insight. „Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case“.
[851] Haaretz. „Black Cube CEO Suspected of Running Crime Organisation – Revealed: The Romania Interrogation“.
[852] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 Juli 2018.
[853] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. Juli 2018.

Laufbahn als „Geheimdienstexperte, Community Builder und Serienunternehmer“ begann[854]. Intellexa Alliance wird auf seiner Website als ein in der EU ansässiges und von der EU reguliertes Unternehmen mit dem Zweck der Entwicklung und Integration von Technologien zur Stärkung der Geheimdienste beschrieben. Zu den Überwachungsanbietern, die Teil der Marketingbezeichnung Intellexa Alliance sind, gehören Cytrox, WiSpear (später umbenannt zu Passitora Ltd), Nexa Technologies (unter der Leitung früherer Amesys-Manager) und Poltrex.

477. All diese Anbieter unterstützen unterschiedliche Systeme. Während Cytrox auf die Extraktion von Daten aus Mobiltelefonen spezialisiert ist, bietet Nexa Technologies die Nutzung globaler mobiler Kommunikationssysteme. WiSpear kann auch Daten aus WLAN-Netzen extrahieren. Die verschiedenen Anbieter in Dilians Allianz ermöglichen somit eine breite Palette von Software und Dienstleistungen, die Intellexa seinen Kunden innerhalb und außerhalb der EU einzeln oder miteinander kombiniert anbieten kann[855].

478. Die Muttergesellschaft von Intellexa Alliance, Thalestris Limited, hat verschiedene Tochtergesellschaften mit Unternehmenspräsenz in Irland, Griechenland, den Britischen Jungferninseln, der Schweiz und Zypern. Sara Aleksandra Hamou, Berichten zufolge die zweite Ex-Frau von Tal Dilian, war Direktorin von Thalestris Limited und Geschäftsführerin einer Tochtergesellschaft mit Sitz in Griechenland[856]. Hamou, die in Polen geboren wurde, besitzt einen zyprischen Reisepass, der von der polnischen Botschaft in Zypern ausgestellt wurde[857].

WISPEAR UND CYTROX

479. Tal Dilian gründete 2013 ein in Zypern registriertes Unternehmen mit dem Namen Aveledo Ltd., das später in WS WiSpear Systems Ltd. und danach in Passitora Ltd. umbenannt wurde[858]. WiSpear hat seinen Sitz in Limassol, Zypern, und verkauft hauptsächlich Ausrüstung und Software für die Lokalisierung und Verfolgung von Personen über ihre Mobiltelefone. In einem Interview mit dem Forbes-Magazin erklärte Dilian die Fähigkeiten der WiSpear-Software, indem er seinen schwarzen Van im Wert von 9 Millionen Dollar zeigte, der in der Lage ist, Geräte in einem Umkreis von 500 Metern zu hacken. WiSpear verfügt auch über Ausrüstung, mit der Daten aus WLAN-Netzen abgefangen werden können[859]. Nach dem Bekanntwerden der Skandale im Zusammenhang mit diesen Produkten wurden die Hauptgeschäftstätigkeiten von Intellexa von Zypern nach Griechenland verlegt.

480. 2017 wurde die Cytrox Holdings Zrt. in Nordmazedonien von Ivo Malinkovski gegründet. Der Ursprung von Cytrox lag jedoch tatsächlich in Tel Aviv, und Malinkovski war nur der führende Kopf des Unternehmens. Nach den Enthüllungen über das Pegasus-Projekt versuchte Malinkovski, alle Spuren zu verwischen, die ihn mit

---

[854] Tal Dilian. About.
[855] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire“.
[856] Thalestris Limited, Jahresbericht und konsolidierte Abschlüsse für den Zeitraum vom 28. November 2019 bis zum 31. Dezember 2020.
[857] ReportersUnited „The Great Nephew and Big Brother“.
[858] Open Corporates, „Passitora Ltd“, https://opencorporates.com/companies/cy/HE318328.
[859] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire“.

Cytrox in Verbindung bringen.

481. Cytrox war Entwickler der Spähsoftware „Predator“. Im Gegensatz zur Spähsoftware „Pegasus“ muss die Zielperson bei Predator auf einen Link klicken, um die Software zu installieren[860]. Als Cytrox kurz vor dem Konkurs stand, rettete Tal Dilian das Unternehmen mit einer Übernahme für weniger als 5 Mio. USD[861]. Cytrox wurde anschließend mit Dilians Unternehmen WiSpear zusammengelegt[862]. Durch diese Übernahme wurde das Arsenal von Intellexa Technologies um die Spähsoftware „Predator“ erweitert. Wie von Lighthouse Reports berichtet, lieferte Intellexa in Zusammenarbeit mit Haaretz und Inside Story die Spähsoftware „Predator“ heimlich und illegal mit einem Privatjet des Unternehmens Cessna an die sudanesische Miliz Rapid Support Forces[863].

482. Nach Angaben von CitizenLab hatten zwei Unternehmen von Cytrox ihren Sitz in Israel (Cytrox EMEA Ltd. und Cytrox Software Ltd.) und eines in Ungarn (Cytrox Holdings Zrt.)[864]. Alle Aktien der Cytrox Holdings Zrt. und der Cytrox EMEA Ltd. – später umbenannt in Balinese Ltd. – wurden auf die Aliada Group Inc. mit Sitz auf den Britischen Jungferninseln übertragen. Der Aliada Group gehört auch WiSpear. Hauptaktionäre der Aliada Group sind Dilian selbst, Oz Liv, Meir Shamir und Avi Rubinstein. Im Dezember 2020 reichte Rubinstein eine Beschwerde gegen seine Mitanteilseigner der Aliada Group wegen der illegalen Verwässerung seiner Anteile ein. Dem Rechtsstreit zufolge wurden mit der Verlagerung von Anteilen auf die Britischen Jungferninseln und später nach Irland israelische und ausländische Ausfuhrkontrollgesetze umgangen[865].

483. Am 16. Dezember 2021 veröffentlichte CitizenLab einen Bericht, aus dem hervorgeht, dass in Armenien, Ägypten, Griechenland, Indonesien, Madagaskar, Oman, Saudi-Arabien und Serbien vermutlich Kunden von Predator festgestellt wurden[866].

AMESYS UND NEXA TECHNOLOGIES

484. Amesys und Nexa Technologies gehören ebenfalls zu Intellexa Alliance und sorgen ihrerseits, wie im Abschnitt über Frankreich beschrieben, für Kontroversen.

POLTREX

485. Poltrex wurde im Oktober 2018 gegründet, mit Intellexa Ltd., registriert auf den Britischen Jungferninseln, als einzigem Aktionär der Gesellschaft. Shahak Avni aus

---

[860] Wissenschaftlicher Dienst des Europäischen Parlaments, „Greece’s Predatorgate. The latest chapter in Europe’s spyware scandal?“.
[861] BalkanInsight, „Wine, Weapons and Whatsapp: A Skopje Spyware Scandal“.
[862] Pitchbook, Cytrox overview.
[863] https://www.lighthousereports.nl/investigation/flight-of-the-predator/
[864] Citizen Lab, „Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware“.
[865] Citizen Lab, „Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware“.
[866] Citizen Lab, „Pegasus vs. Predator. Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware“, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

Israel, Gründer der zypriotischen NCIS Intelligence Services Ltd.[867] und Geschäftspartner von Tal Dilian, wurde im September 2019 als Geschäftsführer von Poltrex eingetragen. Im Oktober 2019 wurden Avni und Dilian Co-Geschäftsführer und der Firmenname wurde von Poltrex in Alchemycorp Ltd. geändert. Ungeachtet der Umbenennung befand sich der Firmensitz weiterhin im Novel Tower, genau wie die Geschäftsräume von WiSpear[868].

486. Als die Ermittlungen im Zusammenhang mit Dilians Spähsoftware-Wagen liefen, wurde das Eigentum an Alchemycorp Ltd. auf Yaron Levgoren., einem Mitarbeiter von Cytrox Holdings, übertragen[869]. Laut seinem LinkedIn-Profil vertritt Levgoren derzeit das zu Intellexa gehörende Unternehmen Apollo Technologies mit Sitz in Griechenland[870].

VERINT/COGNYTE

487. Verint ist ein israelisch-amerikanisches Cyber-Unternehmen mit zahlreichen Tochtergesellschaften in der ganzen Welt. Allein in Europa hat Verint Sitze in Bulgarien, den Niederlanden, Zypern, Deutschland und Frankreich (seit 2021). Verint hatte auch Tochtergesellschaften, die unter dem Namen Cognyte tätig waren. Diese Tochtergesellschaften arbeiten seit 2021, als Verint die Ausgliederung seiner Nachrichten- und Cyberaktivitäten an Cognyte abschloss, unabhängig[871]. Die europäischen Tochtergesellschaften von Cognyte haben ihren Sitz in Zypern (UTX Technologies), Bulgarien (Cognyte Bulgaria EOOD), den Niederlanden (Cognyte Netherlands B.V.), Deutschland (Syborg GmbH, Syborg Grundbesitz GmbH und Syborg Informationsysteme b.h. OHG) und Rumänien (Cognyte Romania S.R.L.)[872].

488. Verint hat Überwachungsinstrumente an mehrere repressive Regierungen verkauft, darunter in Aserbaidschan, Indonesien und Südsudan. Im letzteren Fall setzte der sudanesische Nationale Sicherheitsdienst die Abhörinstrumente von Verint zwischen März 2015 und Februar 2017 gegen Menschenrechtsaktivisten und Journalisten ein. Einer Untersuchung von Amnesty International zufolge ermöglichte der lokale Mobilfunkbetreiber Vivacell Network of the World es dem Nationalen Sicherheitsdienst, alle Telekommunikationsverbindungen im Land abzuhören[873]. Verint beantwortete die Fragen von Amnesty nicht, veröffentlichte aber eine Erklärung, in der erläutert wird, dass Verints unabhängig arbeitende Einheit Cognyte tatsächlich die Verteidigungseinheit sei, während sich Verint ausschließlich mit der Kundenbindung befasse. Nach Angaben von Verint bestand die Trennung mit Cognyte bereits viele Jahre vor der offiziellen Abspaltung im Jahr 2021, um sich von der mutmaßlichen Ausfuhr von Überwachungsinstrumenten in Länder mit schlechter Menschenrechtsbilanz zu distanzieren[874].

---

[867] Philenews, „FILE: The state insulted Avni and Dilian“.
[868] CyprusMail, „Akel says found ‡smoking gun’ linking Cyprus to Greek spying scandal“.
[869] Philenews, „How the spyware scandal in Greece is related to Cyprus“.
[870] https://ca.linkedin.com/in/yaron-levgoren-116948101
[871] Calcalistech, „Verint completes spin-off of its defense activities into new company Cognyte Software“.
[872] https://www.sec.gov/Archives/edgar/data/1824814/000182481421000007/exhibit81.htm.
[873] Haaretz, „Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds“; Amnesty International, „South Sudan: rampant abusive surveillance by NSS instils climate of fear“.
[874] Haaretz, „Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds“.

489. Cognyte hat ebenfalls eine Geschichte von Ausfuhren in Länder mit schlechter Menschenrechtsbilanz. In einer Meta-Untersuchung aus dem Jahr 2021 wurden Kunden in Israel, Serbien, Kolumbien, Kenia, Marokko, Mexiko, Jordanien, Thailand und Indonesien festgestellt[875]. Cognytes in Zypern eingetragenes Tochterunternehmen UTX Technologies hat Berichten zufolge zwischen September 2014 und März 2015 auch Lizenzen für die Ausfuhr von Überwachungssoftware nach Mexiko, in die Vereinigten Arabischen Emirate, nach Nigeria, Israel, Peru, Kolumbien, Brasilien, Südkorea und Thailand erhalten[876]. Vier dieser Länder wurden auch im Meta-Bericht aus 2021 als Cognytes Kunden genannt. Darüber hinaus hat UTX Technologies einen Vertrag mit Bangladesch über ein Web Intelligence System für 2 Mio. USD im Jahr 2019 und über ein zelluläres Tracking-System für 500 000 USD im Jahr 2021 abgeschlossen[877].

490. Am 15. Januar 2023 berichteten Medien, dass Israels Cognyte Software Ltd. einen Monat vor dem Militärputsch im Februar 2021 eine Ausschreibung für den Verkauf seiner Überwachungssoftware an Myanmar erhalten hat. Der Erwerb der Spähsoftware von Cognyte durch Myanmar erfolgte offiziell am 30. Dezember 2020[878].

491. Neben der Ausfuhr in Drittländer hat Cognyte auch den Transport von Ortungsgeräten in die Mitgliedstaaten erleichtert. Über das Unternehmen UTX Technologies, das in Zypern registriert ist, wurde die Gi2-Technologie an eine andere Cognyte-Tochter in Deutschland, Syborg Informationsysteme, geliefert[879]. Diese Gi2-Technologie wurde Berichten zufolge auch an eine Tochtergesellschaft von Verint in Polen „zu Demonstrationszwecken“ geschickt. Die Gi2-Technologie ist in der Lage, sich Zugang zu einem bestimmten Gerät zu verschaffen und kann sich sogar als Besitzer ausgeben und falsche Nachrichten über dasselbe Gerät versenden[880]. Diese Verbringungen fanden zwischen 2013 und 2014 statt. Zu diesem Zeitpunkt waren Verint und Cognyte noch Teil derselben Unternehmensstruktur.

492. UTX Technologies verkaufte 2013 auch Überwachungssysteme an ein französisches Exportunternehmen namens COFREXPORT.[881] Dieses Unternehmen hat seine Tätigkeit eingestellt und ist zum Zeitpunkt der Abfassung dieses Schreibens geschlossen.

493. Wie bei vielen anderen Anbietern von Spähsoftware ist die Unternehmensstruktur von Cognyte aufgrund von Namensänderungen, verschiedenen Abteilungen und durch im Laufe der Zeit erfolgte Spin-offs sehr komplex. Die Tochtergesellschaften von Cognyte zeigen jedoch, dass die EU-Mitgliedstaaten nicht nur als Stützpunkt für den Export von Überwachungsausrüstungen genutzt werden, sondern auch als Wegbereiter für den Verkauf und die Verschiffung von Überwachungsgeräten innerhalb Europas. Israelische Spähsoftware-Unternehmen profitieren somit vom EU-Binnenmarkt und erleichtern den Transport ihrer Ausrüstung sowohl zu ihren eigenen Tochtergesellschaften als auch zu neuen Unternehmen, die in den EU-Mitgliedstaaten registriert sind.

---

[875] Meta, Threat Report on the Surveillance-for-Hire Industry.
[876] Philenews, „Cyprus is a pioneer in software exports“ (Dokumente).
[877] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Records“.
[878] Reuters, „Israel’s Cognyte won tender to sell intercept spyware to Myanmar before coup“ (Dokumente).
[879] https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex81.htm
[880] Philenews, „Cyprus is a pioneer in software exports“ (Dokumente).
[881] Philenews, „Cyprus is a pioneer in software exports“ (Dokumente).

QUADREAM

494. Quadream ist ein israelisches Unternehmen, das von Ilan Dabelstein, einem ehemaligen hohen Beamten des israelischen Nachrichtendienstes, und den ehemaligen NSO-Mitarbeitern Guy Geva und Nimrod Rinsky gegründet wurde. Das Unternehmen ist vor allem für sein Spähsoftware-Produkt Reign bekannt, das angeblich Zero-Click-Exploits verwendet und eine Selbstzerstörungsfunktion enthält, die alle Infektionsspuren löscht. Diese Art von Spähsoftware hat verschiedene Funktionen, wie z. B. Audioaufzeichnung, Standortverfolgung, Suche nach Dateien und Aufnahme von Bildern durch beide Kameras.[882]

495. Laut Citizen Lab und einer Microsoft Threat Intelligence-Analyse arbeiten Quadream-Systeme von Bulgarien, Tschechien, Ungarn, Rumänien, Ghana, Israel, Mexiko, Singapur, den Vereinigten Arabischen Emiraten und Usbekistan aus. Darüber hinaus ergab die Analyse, dass mindestens fünf Zivilgesellschaften in Nordamerika, Zentralasien, Südostasien, Europa und dem Nahen Osten ins Visier genommen werden.[883]

496. In Zypern wurde 2017 ein Unternehmen unter dem Namen InReach registriert. Dieses Unternehmen wurde ausschließlich für die Förderung von Quadream-Produkten wie Reign außerhalb Israels gegründet. Berichten zufolge nutzte Quadream InReach, um seine Produkte an Kunden unter Umgehung der israelischen Ausfuhrkontrollen zu verkaufen. Viele der wichtigsten Mitarbeiter beider Unternehmen haben für die NSO Group, Verint und UT-X Technologies gearbeitet.[884]

497. Nach den Berichten von Citizen Lab und der Microsoft Threat Intelligence-Analyse wurde am 16. April 2023 bekannt gegeben, dass Quadream seine Aktivitäten in Israel eingestellt hat. Laut Haaretz hatte das Unternehmen in den vorangegangenen Monaten mit rückläufigen Umsätzen und Mitarbeiterabgängen zu kämpfen.[885]

CANDIRU

498. Candiru ist ein weiteres in Israel registriertes Unternehmen, das Spähsoftware-Produkte produziert. Es wurde 2014 von Ya'acov Weitzman und Eran Shorer gegründet. Die beiden Gründer haben eine Vergangenheit in der Einheit 8200 des israelischen militärischen Geheimdienstes, und beide waren früher bei der NSO Group

---

[882] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/; https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000?lts=1681386702066

[883] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/

[884] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/; https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000?lts=1681386702066;

[885] https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadream-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000

beschäftigt.[886] Isaac Zack, ein früherer Investor der NSO Group, wurde Hauptaktionär von Candiru. Das Unternehmen verkauft Spähsoftware, um Computer und Server zu hacken.[887] Offengelegte Informationen zu einem Projektvorschlag zeigen, dass Candiru seine Ausrüstung nach der Anzahl gleichzeitiger Infektionen verkauft, also der Anzahl der Zielgeräte, die mit der Spähsoftware zu einem bestimmten Zeitpunkt angegriffen werden können. Beispielsweise erhalten Kunden für 16 Millionen US-Dollar eine unbegrenzte Anzahl von Spyware-Versuchen, können aber nur zehn Zielgeräte gleichzeitig angreifen. Für weitere 1,5 Millionen US-Dollar kann die Kapazität um zusätzliche 15 Geräte erweitert werden.[888]

499. Laut einer Anfrage von TheMarker bietet Candiru nun auch Spähsoftware zum Hacken mobiler Geräte an.[889] Candiru verkauft seine Spionagesoftware ausschließlich an Regierungen, und sein Kundenkreis besteht aus Europa, der ehemaligen Sowjetunion, dem Persischen Golf, Asien und Lateinamerika.[890] Wie im Kapitel über Spanien erwähnt wird, wurden 65 Personen mit Spähsoftware angegriffen; von diesen wurden vier mit Candiru und mindestens zwei Personen sowohl mit Candiru als auch mit Pegasus angegriffen.[891]

500. Wie bei anderen Spähsoftware-Anbietern ist auch für dieses Unternehmen die Verschleierung typisch, und es hat in den letzten Jahren mehrfach seinen Namen geändert. 2017 benannte sich das Unternehmen in DF Associates Ltd., im Jahr 2018 in Grindavik Solutions Ltd., 2019 in Taveta Ltd und jüngst im Jahr 2020 in Saito Tech Ltd um.[892] Aus Gründen der Klarheit wird das Unternehmen in diesem Bericht als Candiru bezeichnet.

501. Ebenso wie die NSO Group wurde Candiru im November 2021 vom US-Handelsministerium auf die schwarze Liste gesetzt. Es wird vermutet, dass der Grund, weswegen Candiru auf die schwarze Liste gesetzt wurde, darin liegt, dass der Geschäftsführer der NSO Group, Shalev Hulio, angeblich ein heimlicher Partner von Candiru war und das Unternehmen mit wichtigen Mittelsmännern in der Welt der Geheimdienste bekannt gemacht hat. Berichten zufolge behauptete Herr Hulio sogar, dass das Produkt von Candiru eigentlich eine Umverpackung von Pegasus sei.[893] Am 1. Juli 2022 identifizierten Sicherheitsforscher eine neuartige Schwachstelle in Chrome, die von Candiru genutzt wurde, um Personen im Libanon, in Palästina, im Jemen und in der Türkei zu hacken.[894] Die Schwachstelle wurde von Google behoben und ist

---

[886] Haaretz „‚ We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers"
[887] Haaretz, „Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed"
[888] Citizen Lab, „Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus"
[889] Haaretz, „Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed".
[890] Citizen Lab, „Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus".
[891] Citizen Lab, „CatalanGate. Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru".
[892] Citizen Lab, „Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus".
[893] Haaretz, „'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers".
[894] TechCrunch, „Spyware maker Candiru linked to Chrome zero-day targeting journalists".

inzwischen auch von Microsoft und Apple behoben worden.[895]

TYKELAB UND RCS LAB

502. Im August 2022 berichtete Lighthouse Reports, dass Tykelab, ein Unternehmen mit Sitz in Rom, das zu RCS Lab gehört, Dutzende von Telefonnetzen, oft auf Inseln im Südpazifik, genutzt hat, um Zehntausende von geheimen „Tracking-Paketen“ in die ganze Welt zu senden, wobei es Menschen in Ländern wie Italien selbst, Griechenland, Nordmazedonien, Portugal, Libyen, Costa Rica, Nicaragua, Pakistan, Malaysia, Irak und Mali ins Visier nahm. Tykelab nutzt Schwachstellen in globalen Telefonnetzen aus, die es Dritten ermöglichen, den Standort von Telefonnutzern einzusehen und möglicherweise deren Anrufe abzuhören, ohne dass auf den Geräten irgendwelche Hinweise auf eine Sicherheitsverletzung hinterlassen werden.[896] In nur zwei Tagen im Juni 2022 sondierte das Unternehmen Netze in fast allen Ländern der Welt.[897] Laut seiner Webseite vereint Tykelab zwanzig Jahre Erfahrung in der Gestaltung, Implementierung und Wartung von Kernnetz-Telekommunikationslösungen mit umfangreichem Fachwissen in der Bereitstellung von Managed Services, kundenbasierter Systemintegration und der Entwicklung mobiler Apps.[898]

503. In der Untersuchung von Lighthouse Report wurde auch die Rolle der Telekommunikationsbranche hervorgehoben, da das Leasing von Telefonnetzzugangspunkten oder „globalen Bezeichnungen“ die Fortsetzung dieses Missbrauchs ermöglicht. Laut GSM Association, der Branchenorganisation, die Mobilfunknetzbetreiber weltweit vertritt, können die Telefonbetreiber nicht immer die Quelle und den Zweck des Verkehrs ermitteln, der über ihre Netze fließt, was es schwierig macht, diesen Praktiken Einhalt zu gebieten.[899]

504. Tykelab ist Teil von RCS Lab, einem italienischen Unternehmen, das für seine Abhörtätigkeiten in Italien und im Ausland bekannt ist; dies wurde durch die Ankündigung eines dritten Unternehmens, Cy4Gate, bekannt, das RCS Lab übernahm. RCS Lab hat Ableger in Frankreich, Deutschland und Spanien[900] sowie eine weitere verdeckte Tochtergesellschaft, Azienda Informatica Italiana, die Abhörsoftware für Android- und iPhone-Geräte baut[901].

DIE SPÄHSOFTWARE HERMIT

505. RCS Lab hat Hermit entwickelt, eine Spähsoftware, mit der sich das Mikrofon des Zieltelefons aus der Ferne aktivieren lässt, Anrufe aufgezeichnet werden können und auf Nachrichten, Anrufprotokolle, Kontaktlisten und Fotos zugegriffen werden kann.[902] Im Juni 2022 deckte die Threat Analysis Group von Google auf, dass von der Regierung unterstützte Akteure, die die Spähsoftware von RCS Lab verwenden, mit den Internetdienstanbietern der Zielpersonen zusammenarbeiteten, um die mobile

[895] The HackerNews, „Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists“.
[896] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[897] https://euobserver.com/digital/155849
[898] http://www.tykelab.it/wp/about/
[899] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[900] https://euobserver.com/digital/155849
[901] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[902] https://www.lighthousereports.nl/investigation/revealing-europes-nso/

Datenverbindung der Zielpersonen zu deaktivieren. Nach der Deaktivierung schickte der Angreifer einen schädlichen Link per SMS, in der die Zielperson aufgefordert wird, eine Anwendung zu installieren, um ihre Datenverbindung wiederherzustellen. Google geht davon aus, dass dies der Grund ist, warum sich die meisten Anwendungen als Anwendungen von Mobilfunkanbietern getarnt haben. Wenn eine Beteiligung eines Internetanbieters nicht möglich ist, werden die Anwendungen als Nachrichten-Anwendungen getarnt. Die Personen, auf die die Spähsoftware vonRCS Lab abzielte, befanden sich in Italien und Kasachstan[903], und die Spähsoftware wurde auch in Rumänien gefunden[904].

506. Ein Bedrohungsforscher der Cybersicherheitsfirma Lookout, Justin Albrecht, erklärte, dass die Installationsmethode von Hermit zwar weniger ausgefeilt sei als die von Pegasus, seine Fähigkeiten aber ähnlich seien. Hermit benötigt zum Hacken eines Geräts einen Telefonnutzer, der auf einen infizierten Link klickt.[905]

507. Laut RCS Lab werden Verkäufe oder Einführungen von Produkten erst nach Erhalt einer behördlichen Genehmigung der zuständigen nationalen Behörden durchgeführt. Die an die Kunden gelieferten Produkte werden in ihren Anlagen installiert, und dem Personal des RCS Lab ist es unter keinen Umständen gestattet, operative Tätigkeiten zur Unterstützung des Kunden durchzuführen oder Zugang zu den verarbeiteten Daten zu erhalten. Aufgrund verbindlicher Vertraulichkeitsvereinbarungen kann RCS Lab keine Einzelheiten zu seinen Kunden offenlegen. Die Cy4gate Group, zu der RCS Lab gehört, ist der Initiative „Global Compact“ der Vereinten Nationen beigetreten und verurteilt daher alle Formen von Menschenrechtsverletzungen. Die Produkte von RCS Lab werden für einen klaren, spezifischen und ausschließlichen Zweck bereitgestellt: Unterstützung der Strafverfolgungsbehörden bei der Verhütung und Bekämpfung abscheulicher Straftaten.[906] Es ist jedoch nicht möglich zu überprüfen, ob die Cy4gate Group, einschließlich RCS Lab, ihre eigenen erklärten Standards einhält.

508. Laut einer im August 2022 veröffentlichten Untersuchung von Lighthouse Reports wurde Tykelabs Überwachungstool Hermit verwendet, um Personen auf der ganzen Welt anzugreifen, darunter in Libyen, Nicaragua, Malaysia, Costa Rica, Irak, Mali, Griechenland und Portugal sowie in Italien selbst.[907]

DECISION SUPPORTING INFORMATION RESEARCH AND FORENSIC (DSIRF)

509. Ein Unternehmen, gegen das das österreichische Justizministerium kürzlich ein Strafverfahren eingeleitet hat, ist die DSIRF GmbH (LLC).[908] DSIRF ist ein 2016 gegründetes österreichisches Unternehmen mit Sitz in Wien und einem Mutterunternehmen in Liechtenstein. Nach eigenen Angaben bietet das Unternehmen

[903] https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

[904] https://www.lighthousereports.nl/investigation/revealing-europes-nso/

[905] https://euobserver.com/digital/155849

[906] https://euobserver.com/digital/155849

[907] Lighthouse Reports, „Revealing Europe’s NSO“, https://www.lighthousereports.nl/investigation/revealing-europes-nso/

[908] DSIRF ist eine Abkürzung für „Decision Supporting Information Research and Forensic“.

maßgeschneiderte Dienstleistungen in den Bereichen Informationsrecherche, Forensik sowie datengestützte Aufklärung für multinationale Unternehmen in den Bereichen Technologie, Einzelhandel, Energie und Finanzen an.[909] DSIRF verkauft offensichtlich an nichtstaatliche Akteure.

510. DSIRF entwickelte Spähsoftware namens Subzero/KNOTWEED, die unter Verwendung von ungeschützten Schwachstellen in Windows und Adobe Reader eingesetzt werden kann und die – laut eigener Werbung – heimlich auf dem Zielgerät installiert werden kann. Nach der Installation übernimmt Subzero die „volle Kontrolle über den Zielcomputer“ und bietet „vollständigen Zugriff auf alle Daten und Passwörter“. Subzero-Kunden können Passwörter extrahieren, Screenshots machen, aktuelle und frühere Standorte ansehen und über eine Webschnittstelle „auf Dateien des Zielcomputers zugreifen, sie herunterladen, ändern und hochladen“. DSIRF bewirbt Subzero als „Cyber-Kriegsführung der nächsten Generation“ und sagt, das Tool sei „für das Cyber-Zeitalter entwickelt“ worden.[910] Im Jahr 2020 schätzte DSIRF den Wert seiner Software Subzero auf 245 Millionen Euro.

511. Die Verbindung zu Russland wird durch Verbindungen mehrerer hochrangiger Mitarbeiter von DSIRF deutlich. Eigentümer von DSIRF ist Peter Dietenberger, ein „Geschäftsmann mit besten Kreml-Kontakten“, der als Türöffner für westliche Unternehmen zu Putins Reich gilt.[911] Dietenberger lebte mehrere Jahre in Russland, hatte ein russisches Unternehmen und mehrere russische Geschäftspartner. Einer seiner russischen Geschäftspartner, Boris Vasilyev, gehörte auch dem Verwaltungsrat von DSIRF an. DSIRF nennt mehrere Referenzen für seine Firma und Produkte: Michael Harms (Geschäftsführer des Ost-Ausschusses der Deutschen Wirtschaft), Stephan Fanderl (Vorsitzender des Vorstands von Galeria Karstadt Kaufhof, der Walmart nach Russland bringen wollte), Christian Kremer (ehemaliger Präsident von BMW in Russland und CEO von Russian Machines, der seit 2018 von den USA sanktioniert wird) und Florian Schneider (Partner der großen Anwaltskanzlei Dentons in Moskau).[912] Russian Machines, ein Unternehmen im Eigentum des Oligarchen Oleg Deripaska, soll die Dienste von DSIRF in Anspruch nehmen. Der mächtige lokale Unternehmer Siegfried „Sigi“ Wolf, der den ehemaligen Bundeskanzler Sebastian Kurz in Wirtschaftsfragen beriet, gilt als Vertrauter von Deripaska.[913] Auch Jan Marsalek, ein mutmaßlicher Straftäter, der aufgrund eines Interpol-Haftbefehls wegen Betrugsvorwürfen in Milliardenhöhe und anderen Finanz- und Wirtschaftsdelikten gesucht wird, ist beteiligt. Im August 2018 erhielt er eine E-Mail von Florian Stermann (Generalsekretär der Österreichisch-Russischen Freundschaftsgesellschaft, der in Ermittlungen der Staatsanwaltschaft als „Vertrauter“ der FPÖ angesehen wurde)[914] mit einer Unternehmenspräsentation von DSIRF. Im Jahr 2013 versuchte Marsalek angeblich, Spähsoftware des italienischen Unternehmens Hacking Team an Grenada zu

[909] https://dsirf.eu/about/
[910] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
[911] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
[912] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
[913] https://www.derstandard.at/story/2000131301583/causa-marsalek-die-verbindungen-einer-spionagefirma-werfen-fragen-auf
[914] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html

verkaufen. Er soll sich derzeit unter Aufsicht des FSB, des russischen Geheimdienstes, in Moskau verstecken.[915]

512. Im Juli 2022 fand Microsoft heraus, dass Subzero im Rahmen unautorisierter, bösartiger Aktivitäten, d.h. für Angriffe auf Anwaltskanzleien, Banken und strategische Beratungsunternehmen in Österreich, dem Vereinigten Königreich und Panama verwendet wurde.[916] In Österreich gibt es derzeit keine Rechtsgrundlage für den unbefugten Einsatz von Spähsoftware wie Subzero durch Behörden, und auch der Einsatz durch ein privates Unternehmen gegen ein anderes Unternehmen wäre illegal. Im Anschluss an die Microsoft-Veröffentlichung erstattete die österreichische nichtstaatliche Organisation im Bereich der digitalen Rechte Epicenter.works am 28. Juli 2022 Strafanzeige gegen DSIRF bei der Staatsanwaltschaft Wien wegen unrechtmäßigen Zugriffs auf ein Computersystem, Datenbeschädigung, Beeinträchtigung der Funktionsfähigkeit von Computersystemen, betrügerischen Missbrauchs der Datenverarbeitung, krimineller Organisation und Verstoßes gegen das Außenwirtschaftsgesetz in Bezug auf Güter mit doppeltem Verwendungszweck.[917] Am 7. Oktober 2022 teilte das österreichische Bundesministerium für Arbeit und Wirtschaft mit, dass es DSIRF keine Ausfuhrgenehmigung erteilt habe[918], und nach Angaben des österreichischen Bundesministeriums für Justiz hat die Staatsanwaltschaft Wien ein Ermittlungsverfahren gegen DSIRF eingeleitet[919]. Der gegen Ziele in Österreich gerichtete Einsatz der Spähsoftware Subzero bedeutet, dass eine private oder öffentliche Stelle in Österreich die Software illegal eingesetzt hat, dass sie von einem ausländischen Akteur verwendet wurde und DSIRF gegen Ausfuhrbeschränkungen verstoßen hat oder dass sie in einen anderen Mitgliedstaat exportiert und von dort aus – legal oder illegal – gegen ein österreichisches Ziel gerichtet eingesetzt wurde. Die entsprechenden Ermittlungen sind noch nicht abgeschlossen.

FinFisher

513. Ein wichtiger Punkt in diesem Bericht ist auch die strafrechtliche Untersuchung und der Konkurs von FinFisher, einem ehemaligen Spähsoftware-Unternehmen mit Sitz in München, Deutschland. FinFisher ist ein im Jahr 2008 gegründetes Unternehmensnetz, das ursprünglich starke Verbindungen zum britischen Unternehmensnetz, das unter der Marke Gamma tätig ist, hatte. FinFisher warb für seine Spähsoftware als „komplettes IT-Eingriffs-Portfolio“, wobei seine Software in Dutzenden von Ländern auf der ganzen Welt[920] eingesetzt wurde, darunter 11 EU-Mitgliedstaaten[921] und 13 „nicht-freie“

---

[915] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/; https://www.dw.com/en/wanted-wirecard-executive-jan-marsalak-reportedly-hiding-in-moscow/a-61440213

[916] https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

[917] https://en.epicenter.works/document/4236

[918] Antwort von Martin Kocher, österreichischer Bundesminister für Digitalisierung und Wirtschaftsstandort, auf schriftliche parlamentarische Anfragen von Stephanie Krisper, 7. Oktober 2022, Referenz 2022-0.575.143, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml

[919] Antwort von Alma Zadić, Bundesministerin für Justiz, auf schriftliche parlamentarische Anfragen von Stephanie Krisper, 7. Oktober 2022, Referenz 2022-0.575.216, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml.

[920] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; https://wikileaks.org/spyfiles4/customers.html

[921] Belgien, Deutschland, Estland, Italien, die Niederlande, Rumänien, die Slowakei, Slowenien, Spanien, Tschechien und Ungarn.

Länder[922].

514. Im Jahr 2017 tauchte das Produkt FinSpy von FinFisher in der Türkei auf einer gefälschten Version einer Website für die Mobilisierung der türkischen Opposition auf. Die Software war als herunterladbare App getarnt, die Teilnehmern von regierungskritischen Demonstrationen empfohlen wurde.[923] FinFisher selbst bewarb seine Produkte als ausschließlich zur Kriminalitätsbekämpfung bestimmt. Im Jahr 2019 wurde von der Gesellschaft für Freiheitsrechte, Reporter ohne Grenzen, dem Blog netzpolitik.org und dem European Center for Constitutional and Human Rights eine Strafanzeige gegen FinFisher wegen Export seiner Spähsoftware ohne die erforderliche Ausfuhrgenehmigung des deutschen Bundesamtes für Wirtschaft und Ausfuhrkontrolle erstattet. Damit habe das Unternehmen gegen die Verordnung über Güter mit doppeltem Verwendungszweck und die entsprechenden deutschen Rechtsvorschriften verstoßen. Im Anschluss an die Anzeige hat die Staatsanwaltschaft München gegen FinFisher ermittelt und im Oktober 2020 15 Geschäftsräume der FinFisher-Unternehmensgruppe in Deutschland und Rumänien sowie Privatwohnsitze durchsucht. Im Jahr 2021 genehmigte das Amtsgericht München die Pfändung der Bankkonten von FinFisher durch die Staatsanwaltschaft, um die Einziehung illegal erzielter Gewinne nach einer möglichen Verurteilung durch FinFisher sicherzustellen. Jedoch meldete FinFisher im Februar 2022 Insolvenz an. Der Geschäftsbetrieb wurde eingestellt, das Büro wurde geschlossen und alle 22 Mitarbeiter wurden entlassen.[924] Die strafrechtlichen Ermittlungen gegen die für die Aktivitäten von FinFisher verantwortlichen Personen sind noch nicht abgeschlossen.

III. Kapazität der Europäischen Union für Reaktionen

515. Einige Regierungen haben EU-Bürger mit leistungsfähiger und in hohem Maße invasiver und in die Privatsphäre eingreifender Spähsoftware angegriffen und damit ihr Recht auf Überwachung im Falle einer Gefahr für die nationale Sicherheit missbraucht. Dies stellt eine Bedrohung für die Demokratie, die Rechtsstaatlichkeit und die Grundrechte der einzelnen Bürgerinnen und Bürger dar. Die EU hat nur wenige Befugnisse, um gegen diese Bedrohungen vorzugehen, und sie erweist sich als schlecht gerüstet gegenüber möglichen kriminellen Handlungen der nationalen Behörden, selbst wenn diese die EU selbst betreffen. Gemäß den Verträgen fällt die nationale Sicherheit in die ausschließliche Zuständigkeit der Mitgliedstaaten, ihr Handeln muss aber auf jeden Fall den Grundrechten und demokratischen Normen entsprechen, die im EU-Recht verankert sind. Auch politische Faktoren schränken die Handlungsbefugnisse der EU ein. Die Kommission als Hüterin der EU-Verträge hat ihre Bemühungen, das EU-Recht unter Einsatz der ihr zur Verfügung stehenden Rechtsinstrumente durchzusetzen, nicht maximal vorangetrieben. Die Kommission neigt dazu, ihre Befugnisse sehr eng, als fast ausschließlich die korrekte Umsetzung des EU-Rechts in nationales Recht

[922] Ägypten, Äthiopien, Angola, Bahrain, Bangladesch, Gabun, Jordanien, Kasachstan, Katar, Myanmar, Oman, Saudi-Arabien und die Türkei.
[923] https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/
[924] https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/; https://edri.org/our-work/criminal-complaint-against-illegal-export-of-surveillance-software-is-making-an-impact-the-finfisher-group-of-companies-ceases-business-operations-after-its-accounts-are-seized-by-public-prosecutor/; https://netzpolitik.org/wp-upload/2022/03/2022-02-08_AG-Muenchen_Insolvenzbekanntmachung_FinFisher-Labs-GmbH.txt

betreffend, auszulegen. Die Kommission ist der Auffassung, dass die Bekämpfung von Verstößen gegen EU-Recht in die alleinige Verantwortung der nationalen Behörden fällt. Angesichts schwerwiegender Verstöße gegen die Rechtsstaatlichkeit und die Grundrechte wird diese Haltung, die keine Grundlage in den EU-Verträgen hat, sehr problematisch. Auch wenn Subsidiarität und Aufteilung der Zuständigkeiten eine Säule des EU-Rechts sind, sollte dies nicht zu Straflosigkeit für Regierungen führen, die EU-Bürger für politische Zwecke mit Spähsoftware überwachen. Im Folgenden werden die Befugnisse untersucht, über die die Organe der EU verfügen. Das Parlament, die Kommission und der Rat haben die Befugnis und die Pflicht, Gesetze zu erlassen und Regelungen vorzunehmen sowie diese durchzusetzen, und sie müssen dies mit Nachdruck und Ehrgeiz tun und dabei die Verteidigung unserer Demokratie über kurzfristige politische Überlegungen stellen.

Europäische Kommission

516. Nach Presseberichten über den Einsatz von Spähsoftware in den Mitgliedstaaten und Fragen des PEGA-Ausschusses hat die Kommission in ihrer Reaktion auf den Spähsoftware-Skandal zunächst nur Schreiben an die Regierungen Polens, Ungarns, Spaniens, Griechenlands, Zyperns und Frankreichs gerichtet, in denen sie um Klarstellung ersuchte. Es scheint jedoch, dass dieser Ermahnung durch die Kommission keine weiteren Maßnahmen folgten. Es stimmt, dass die Kommission streng genommen keine Befugnisse hat, im Bereich der nationalen Sicherheit tätig zu werden. Wie die Kommission in diesen Schreiben jedoch selbst betont, sollte der Begriff „nationale Sicherheit“ nicht als unbegrenzte Ausnahmeregelung von den europäischen Gesetzen und Verträgen interpretiert werden und zu einem Bereich der Gesetzlosigkeit werden. Es ist allerdings Sache der Mitgliedstaaten, „nachzuweisen, dass die nationale Sicherheit im vorliegenden Fall gefährdet wäre“. In Beantwortung der Frage, welche Maßnahmen die Kommission ergreifen wird, wenn die nationalen Behörden Vorwürfe der illegalen Spionage nicht eingehend prüfen, verweist die Kommission lediglich auf den Europäischen Gerichtshof und auf Artikel 47 der Charta, der das Recht auf einen wirksamen Rechtsbehelf vor einem Gericht vorsieht. Es scheint keine politische Bereitschaft zum Handeln zu geben.

517. Darüber hinaus richtete die Kommission am 21. Dezember 2022 ein allgemeines Schreiben an alle Mitgliedstaaten, in dem sie Informationen über die Verwendung von Spähsoftware durch die nationalen Behörden und den Rechtsrahmen für eine solche Verwendung für die Zwecke einer Bestandsaufnahme der Situation in den Mitgliedstaaten und die Prüfung des Zusammenspiels mit dem Unionsrecht anforderte.[925] Die Kommission stellte spezifische Fragen, u. a. zu dem Zweck der Verwendung von Spähsoftware, den dazu befugten Behörden, der nationalen Definition der nationalen Sicherheit, den einschlägigen Rechtsvorschriften, die die Verarbeitung von Daten zu Zwecken der nationalen Sicherheit regeln, Garantien, vorherige Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsbehörde, Aufsicht und Meldung, mit einer Frist zur Stellungnahme bis zum 31. Januar 2023. Am 28. März 2023 erklärte Kommissar Reynders gegenüber dem PEGA-Ausschuss, dass eine große Mehrheit der Mitgliedstaaten geantwortet habe, die Kommission jedoch noch dabei sei, die Antworten der Mitgliedstaaten für die Bestandsaufnahme zu sammeln, und dass sie

[925] Schreiben der GD JUST an die Mitgliedstaaten. Ref. Ares(2022)8885417 vom 21. Dezember 2022.

die Antworten sorgfältig prüfen werde. Auf der Grundlage dieser Bestandsaufnahme werde die Kommission über ihre Optionen für die Verwendung von Spähsoftware in den Mitgliedstaaten nachdenken. Für die Bewertung durch die Kommission sei jedoch aufgrund des sich weiterentwickelnden und sensiblen Charakters der Bewertung kein spezifisches Enddatum vorgesehen. Die Kommission wies ferner darauf hin, dass sie die Feststellungen des PEGA-Ausschusses sehr genau verfolgen werde.

518. Im Unterschied zu den USA, die auf die Enthüllungen reagiert haben, indem sie Unternehmen auf die schwarze Liste gesetzt, Untersuchungen, auch in EU-Gebieten, durchgeführt und eine Durchführungsverordnung erlassen haben, die den Erwerb von kommerzieller Spähsoftware durch US-Bundesbehörden verbietet, hat die Kommission bisher weder eine Analyse der Situation noch eine Bewertung der auf dem Spähsoftware-Markt in der EU tätigen Unternehmen vorgenommen. Es gibt keine offensichtlichen rechtlichen Einwände gegen die Durchführung einer solchen Analyse. Es ist bemerkenswert, dass die zahlreichen Nachweise die Kommission noch immer nicht zu sinnvollen Maßnahmen veranlasst haben. Ihre Trägheit kommt einer Mittäterschaft bei Menschenrechtsverletzungen und Pflichtvernachlässigung gleich.

519. Die EU verfügt über mehrere Gesetze, die als Regulierungsinstrumente in Bezug auf Spähsoftware dienen können. Neben Gesetzen zum Schutz der Rechte der Bürger, wie den Gesetzen zum Datenschutz und zum Schutz der Privatsphäre in der Kommunikation (DSGVO, Datenschutzrichtlinie für elektronische Kommunikation[926]), gibt es Gesetze zur Ausfuhr (Verordnung über Güter mit doppeltem Verwendungszweck) und zur Vergabe öffentlicher Aufträge. Die Möglichkeiten für die Durchsetzung werden von der Kommission als Hüterin der Verträge jedoch nicht voll ausgeschöpft. Sie beschränkt sich in der Regel darauf, zu überprüfen, ob ein Mitgliedstaat EU-Rechtsvorschriften ordnungsgemäß in nationales Recht umgesetzt hat. Dies sagt jedoch sehr wenig über die tatsächliche Situation vor Ort aus. So scheint der Bericht der Kommission über die Durchführung der Verordnung über Güter mit doppeltem Verwendungszweck[927] zu dem Schluss zu kommen, dass die Umsetzung gut vorankommt, während es zahlreiche Beweise dafür gibt, dass sie in der Praxis schwach und lückenhaft ist und in einigen Ländern sogar absichtlich so erfolgt. Die Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation und die daraus abgeleitete Rechtsprechung sind unzureichend. Die Kommission weist darauf hin, dass die Mitgliedstaaten für die Anwendung und Durchsetzung zuständig sind, aber sie ergreift keine Maßnahmen, wenn die Mitgliedstaaten diese Aufgaben nicht erfüllen. Ohne eine ordnungsgemäße und sinnvolle Durchsetzung sind die EU-Rechtsvorschriften unwirksam und schaffen viel Raum für die illegale Nutzung von Spähsoftware.

520. Die Richtlinie zum Datenschutz bei der Strafverfolgung war dazu bestimmt, hohe Datenschutzstandards zu bieten und den freien Datenverkehr in den Bereichen Strafverfolgung und Strafjustiz sicherzustellen. Die Richtlinie musste in nationales Recht umgesetzt werden, wobei den Mitgliedstaaten ein weiter Ermessensspielraum eingeräumt wurde. Heute ist offenkundig, dass sich die Umsetzung von Mitgliedstaat zu

[926] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201 vom 31.7.2002, S. 37).
[927] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

Mitgliedstaat unterscheidet, insbesondere im Bereich der Rechte betroffener Personen. Die Kommission sollte dringend die Umsetzung in allen Mitgliedstaaten bewerten und die schwerwiegendsten Mängel ermitteln. Die Kommission sollte für die Mitgliedstaaten konkrete Leitlinien für die Umsetzung der Richtlinie entwickeln, damit die EU-Standards in der gesamten Union eingehalten werden. Darüber hinaus sollte die Kommission erforderlichenfalls Vertragsverletzungsverfahren einleiten, wenn die Richtlinie nicht ordnungsgemäß umgesetzt wurde und der Mitgliedstaat nicht bereit ist, die Mängel zu beheben.

Europäisches Parlament

521. Das Europäische Parlament hat den Untersuchungsausschuss PEGA eingesetzt, der im Rahmen seiner Befugnisse und seines Mandats gewissenhaft und effizient arbeitet. Er ist jedoch nicht befugt, Zeugen vorzuladen oder unter Eid zu vernehmen, und er hat keinen Zugang zu Verschlusssachen. Ihm fehlen die vollen Ermittlungsbefugnisse, über die die meisten nationalen Parlamente verfügen. Darüber hinaus ist der Einfluss der nationalen Regierungen bei den Beratungen des PEGA-Ausschusses häufig präsent, was gelegentlich ein Hindernis für gründliche, völlig unabhängige und objektive Untersuchungen darstellt. Es ist ziemlich beunruhigend, dass das Europäische Parlament nicht über die vollen Ermittlungsbefugnisse verfügt, wenn einige seiner eigenen Mitglieder mit Spähsoftware überwacht wurden.

Europäischer Rat und Rat der Europäischen Union

522. Obwohl die nationalen Regierungen behaupten, der Spähsoftware-Skandal sei eine rein nationale Angelegenheit, wurde er tatsächlich im Rat der Europäischen Union erörtert, und die nationalen Regierungen haben beschlossen, den Fragebogen des Europäischen Parlaments gemeinsam zu beantworten.[928] Damit haben sie voll und ganz anerkannt, dass es sich in der Tat um eine Angelegenheit des Rates handelt.

523. Bislang hat der Europäische Rat weder öffentlich noch substanziell auf den Skandal reagiert. Einige seiner Mitglieder haben ein Interesse an der Angelegenheit, da sie möglicherweise selbst in die illegalen Hacks verwickelt sind, oder sie möchten einfach, dass die EU in diesem Gebiet schwach und machtlos bleibt.

524. Selbst wenn letztlich ein rechtswidriges oder kriminelles Verhalten nachgewiesen werden sollte, könnten Mitglieder nationaler Regierungen nicht angeklagt oder zum Rücktritt von Ihren EU-Posten gezwungen werden. Dies bedeutet, dass Personen, die sich solcher Handlungen schuldig gemacht haben, weiterhin ungestraft in Einrichtungen der EU sitzen und Entscheidungen treffen können, die alle europäischen Bürger betreffen.

Europol

525. Europol verfügt über keine autonomen operativen Befugnisse und kann gemäß Artikel 88 Absatz 3 AEUV nicht ohne die Zustimmung und die Zusammenarbeit des betroffenen Mitgliedstaats bzw. der betroffenen Mitgliedstaaten handeln, wobei die Anwendung von Zwangsmaßnahmen ausschließlich den zuständigen nationalen

[928] Entwurf eines Schreibens des Generalsekretariat des Rates an die Delegationen, 26. September 2022.

Behörden vorbehalten bleibt. Dies stellt ein Problem dar, wenn es eindeutige Beweise für kriminelle Handlungen – wie Cyberkriminalität, Korruption und Erpressung – gibt, die nationalen Behörden aber nicht ermitteln. Europol hat vor Kurzem neue Befugnisse erhalten, die es der Agentur erlauben, proaktiv eine Ermittlung vorzuschlagen, auch wenn es sich um eine Straftat handelt, die nur in einem Mitgliedstaat begangen wurde[929], hat aber bisher nicht von diesen Befugnissen Gebrauch gemacht.

526. Am 28. September 2022 richtete PEGA ein Schreiben an Europol[930], in dem der Ausschuss Europol nachdrücklich auffordert, von seinen neuen Befugnissen gemäß Artikel 6 der Europol-Verordnung[931] Gebrauch zu machen. In einem Antwortschreiben vom 13. Oktober 2022[932] teilte Europol mit, dass es sich mit fünf Mitgliedstaaten in Verbindung gesetzt habe, um festzustellen, ob auf nationaler Ebene relevante Informationen für Europol zur Verfügung stehen und ob eine strafrechtliche Ermittlung (oder stattdessen eine andere Untersuchung nach den geltenden Bestimmungen des nationalen Rechts) läuft oder geplant ist. Am 11. April 2023 erklärte Europol in einem Schreiben an PEGA, dass ihre Schreiben an Griechenland, Ungarn, Bulgarien, Spanien und Polen übermittelt worden seien. Laut Europol hatte keiner der fünf Mitgliedstaaten in seiner Antwort auf die Schreiben von Europol relevante und für Europol verfügbare Informationen. Bis Oktober 2022 hatte einer der fünf Mitgliedstaaten Europol bestätigt, dass strafrechtliche Ermittlungen unter der Aufsicht der zuständigen Justizbehörden eingeleitet worden seien, was auch von Eurojust überprüft worden sei. Bis Dezember 2022 hatte ein zweiter Mitgliedstaat Europol mitgeteilt, dass im Zusammenhang mit der mutmaßlichen rechtswidrigen Verwendung der Software Pegasus ein Strafverfahren eingeleitet worden und inzwischen von den zuständigen Justizbehörden dieses Landes abgeschlossen worden sei. Ein dritter Mitgliedstaat teilte Europol mit, dass in einem Fall auf regionaler Ebene ein Vorverfahren eingeleitet worden sei, und erkundigte sich, ob Europol über Informationen über die Verwendung der Software Pegasus in dem betreffenden Land verfügt, die für das Vorverfahren relevant sind. Ein vierter Mitgliedstaat teilte Europol mit, dass keine strafrechtlichen Ermittlungen liefen oder geplant seien, dass jedoch gerichtliche Ermittlungen eingeleitet worden seien. Bis April 2023 hatte der fünfte Mitgliedstaat Europol erklärt, dass sich aus der Konsultation der zuständigen Behörden des Landes keine für Europol relevanten Informationen über den rechtswidrigen Einsatz von eingreifender Überwachungs- und Abhörsoftware im Zusammenhang mit Vorfahren der Staatsanwaltschaft ergeben hätten. Es ist nicht bekannt, ob die oben genannten Strafverfahren zweier Mitgliedstaaten, das Vorverfahren eines Mitgliedstaats, die gerichtlichen Ermittlungen eines Mitgliedstaats und das Vorverfahren der Staatsanwaltschaft eines weiteren Mitgliedstaats den Missbrauch von Spähsoftware durch die Regierungen von EU-Mitgliedstaaten oder

[929] Verordnung (EU) 2022/991 des Europäischen Parlaments und des Rates vom 8. Juni 2022 zur Änderung der Verordnung (EU) 2016/794 hinsichtlich der Zusammenarbeit Europols mit privaten Parteien, der Verarbeitung personenbezogener Daten durch Europol zur Unterstützung strafrechtlicher Ermittlungen und der Rolle von Europol in Forschung und Innovation (ABl. L 169 vom 27.6.2022, S. 1).
[930] https://twitter.com/EP_PegaInquiry/status/1576855144574377984
[931] „[D]er Exekutivdirektor [kann] in den Fällen, in denen er der Auffassung ist, dass strafrechtliche Ermittlungen zu einer bestimmten Straftat eingeleitet werden sollten, die zwar nur einen Mitgliedstaat betrifft, aber ein gemeinsames Interesse verletzt, das Gegenstand einer Politik der Union ist, den zuständigen Behörden des betreffenden Mitgliedstaats über seine nationale Stelle die Einleitung, Durchführung oder Koordinierung einer strafrechtlichen Ermittlung vorschlagen.“
[932] Akte Nr. 1260379.

durch Drittländer betreffen.

527. Die EU erweist sich als ziemlich machtlos gegenüber möglichen kriminellen Handlungen der nationalen Behörden, selbst wenn diese die EU betreffen.

528. Paradoxerweise untersuchen die USA im Gegensatz zu Europol aktiv den Einsatz von Spähsoftware in der EU. Am 5. November 2022 wurde berichtet, dass das FBI Athen besuchte, um zu untersuchen, „wie weit sich die illegale Überwachung ausgebreitet hat und wer mit ihr gehandelt hat.“[933] Darüber hinaus erließ US-Präsident Biden im März 2023 eine Executive Order, die den Einsatz von Spähsoftware durch US-Bundesbehörden weitgehend verbietet. Einige Tage später bekundeten andere Länder, darunter Frankreich und Dänemark, ihr Engagement für eine internationale Zusammenarbeit bei diesem Thema.

Europäische Justiz

529. Der EuGH und der EGMR spielen eine wichtige Rolle bei der Verteidigung von Demokratie, Rechtsstaatlichkeit und Grundrechten. Sie können jedoch nur auf eine Beschwerde oder eine vorgerichtliche Frage hin tätig werden. Die Verfahren sind sehr langwierig und bieten in Einzelfällen kaum konkrete Abhilfe. Im Laufe der Jahre haben die Gerichte eine umfangreiche einschlägige Rechtsprechung geschaffen und beispielsweise Standards für die Überwachung festgelegt. Die Gerichte verfügen jedoch nicht über die Mittel, um für die Durchsetzung ihrer Urteile zu sorgen. Bislang wurde dem EGMR eine Beschwerde über den unrechtmäßigen Einsatz von Spähsoftware vorgelegt.[934] Der Weg zu den Gerichten in Straßburg oder Luxemburg ist jedoch oft lang, kostspielig und umständlich, da zunächst alle Möglichkeiten der nationalen Gerichtsverfahren ausgeschöpft werden müssen. Dies gilt insbesondere dann, wenn nationale Staatsanwälte oder Richter einen Fall nicht annehmen oder ablehnen. Die Hürde für die Zulässigkeitsprüfung ist hoch.

Die Bürgerbeauftragte

530. Am 28. November 2022 stellte die Bürgerbeauftragte der EU fest, dass die Kommission die Risiken in Bezug auf die Menschenrechte nicht ausreichend geprüft hat, bevor sie afrikanischen Ländern beim Aufbau von Kapazitäten für die Überwachung Unterstützung bereitgestellt hat, insbesondere im Zusammenhang mit dem Nothilfe-Treuhandfonds der EU für Afrika (EUTF Afrika). Die Feststellungen folgten auf eine Beschwerde mehrerer zivilgesellschaftlicher Organisationen. In Niger wurden aus dem Fonds trotz Unterdrückung von Aktivisten im Land 11,5 Mio. EUR für die Lieferung von Überwachungsausrüstung bereitgestellt, darunter Überwachungssoftware, ein Abhörzentrum und ein IMSI-Catcher[935]. Um die festgestellten Mängel zu beheben, schlug die Bürgerbeauftragte Verbesserungen vor, um sicherzustellen, dass für künftige EUTFA-Projekte eine vorherige Folgenabschätzung in Bezug auf Menschenrechte

[933] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ
[934] Klage von Koukakis vor dem Europäischen Gerichtshof für Menschenrechte, 27. Juli 2022.

[935] https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf

durchgeführt wird.

Andere EU-Einrichtungen

531. Der Europäische Datenschutzausschuss, der Europäische Datenschutzbeauftragte, der Europäische Rechnungshof und Eurojust verfügen nur über wenige Befugnisse, um im Falle der unrechtmäßigen Verwendung von oder des Handels mit Spähsoftware durch die Regierungen von Mitgliedstaaten Untersuchungen vorzunehmen oder einzugreifen. Einige ihrer Mitglieder könnten in der Tat in die Skandale in ihrem Herkunftsmitgliedstaat verwickelt sein. Dies kann Auswirkungen auf die Funktionsweise und die Integrität dieser Einrichtungen der EU haben. Die Europäische Staatsanwaltschaft könnte möglicherweise eingreifen, wenn EU-Gelder in irgendeiner Weise involviert sind.

BEGRÜNDUNG

Europas Watergate

Im Sommer 2021 veröffentlichte das Pegasus-Projekt, ein Konsortium von investigativen Journalisten, Nichtregierungsorganisationen und Forschern, eine Liste von 50 000 Personen, die mit Söldner-Spähsoftware überwacht worden waren. Darunter befanden sich Journalisten, Anwälte, Staatsanwälte, Aktivisten, Politiker und sogar Staatsoberhäupter. Am dramatischsten dürfte der Fall Jamal Khashoggi sein, der saudische Journalist, der 2018 wegen seiner Kritik am saudischen Regime brutal ermordet wurde. Es standen aber auch viele europäische Zielpersonen auf der Liste. Einige wurden von Akteuren von außerhalb der EU ins Visier genommen, andere aber auch von ihren eigenen nationalen Regierungen. Die Enthüllungen stießen weltweit auf Empörung.

Der Skandal wurde schnell als „Europas Watergate“ bezeichnet. Doch erinnert der Spähsoftware-Skandal von heute weniger an den politischen Thriller „Die Unbestechlichen“ über den Einbruch in das Watergate-Gebäude im Jahr 1972 als an den beklemmenden Film „Das Leben der Anderen“, der die Überwachung der Bürger durch das totalitäre kommunistische Regime abbildet. Heute ist ein digitaler Einbruch mit Spähsoftware weitaus ausgefeilter und invasiver und hinterlässt kaum Spuren. Der Einsatz von Spähsoftware geht weit über die herkömmliche Überwachung einer Person hinaus. Er bietet den ausspionierenden Akteuren totalen Zugriff und vollständige Kontrolle. Im Gegensatz zum klassischen Abhören ermöglicht Spähsoftware nicht nur eine Echtzeitüberwachung, sondern auch den vollständigen, rückwirkenden Zugriff auf in der Vergangenheit erstellte Dateien und Nachrichten sowie auf Metadaten über zurückliegende Kommunikationen. Die Überwachung kann sogar aus der Ferne erfolgen, überall auf der Welt in jedem Land. Spähsoftware kann im Wesentlichen dazu dienen, ein Smartphone zu hacken und all seine Inhalte, einschließlich Dokumente, Bilder und Nachrichten, zu extrahieren. Das so gewonnene Material kann nicht nur dazu verwendet werden, um Handlungen zu beobachten, sondern auch um die Opfer zu erpressen, zu diskreditieren, zu manipulieren und einzuschüchtern. Der Zugriff auf das System des Opfers kann manipuliert werden, und es können frei erfundene Inhalte implantiert werden. Mikrofon und Kamera können aus der Ferne aktiviert werden und verwandeln das Gerät in einen Spion im eigenen Haus. Das Opfer bekommt nichts davon mit. Spähsoftware hinterlässt nur wenige Spuren auf dem Gerät des Opfers, und selbst wenn sie entdeckt wird, ist es nahezu unmöglich nachzuweisen, wer für den Angriff verantwortlich war.

Der Missbrauch von Spähsoftware verletzt nicht nur das Recht auf Privatsphäre natürlicher Personen. Er untergräbt auch heimlich die Demokratie und die demokratischen Institutionen. Er schaltet die Opposition und Kritiker stumm, verhindert Überprüfungen und hat eine abschreckende Wirkung auf die freie Presse und die Zivilgesellschaft. Er dient auch dazu, Wahlen zu manipulieren. Der Begriff „Söldner-Spähsoftware“ beschreibt sehr gut den Charakter des Produkts und der Industrie. Sogar gescheiterte Versuche, ein Smartphone mit Spähsoftware zu infizieren, haben politische Auswirkungen und können sowohl dem Einzelnen als auch der Demokratie Schaden zufügen. Die Teilnahme am öffentlichen Leben wird unmöglich, wenn die Gewissheit fehlt, frei und unbeobachtet zu sein.

Der Spähsoftware-Skandal ist keine Folge isolierter nationaler Missbrauchsfälle, sondern eine ausgewachsene europäische Angelegenheit. Regierungen von EU-Mitgliedstaaten haben

Spähsoftware genutzt, um ihre Bürger zu politischen Zwecken auszuspionieren und Korruption und kriminelle Aktivitäten zu vertuschen. Einige gingen sogar noch weiter und haben Spähsoftware in ein System eingebaut, das gezielt für autoritäre Regierungsstrukturen entwickelt wurde. Regierungen anderer Mitgliedstaaten haben zwar keinen Missbrauch von Spähsoftware begangen, aber den verborgenen Handel mit Spähsoftware erleichtert. Europa ist zu einem attraktiven Ort für Söldner-Spähsoftware geworden. Es war Drehscheibe für Exporte in Diktaturen und Unterdrückungsregime wie Libyen, Ägypten und Bangladesch, wo die Spähsoftware gegen Menschenrechtsaktivisten, Journalisten und Regierungskritiker eingesetzt wurde.

Der Missbrauch von Spähsoftware bedeutet eine schwere Verletzung aller Werte der Europäischen Union und stellt die Widerstandsfähigkeit der Demokratie und Rechtsstaatlichkeit in Europa auf die Probe. In den letzten Jahren hat die EU ihre Kapazität zur Reaktion auf externe Bedrohungen unserer Demokratie, sei es Krieg, Desinformationskampagnen oder politische Einmischung, sehr schnell ausgebaut. Im Gegensatz dazu bleibt die Fähigkeit, auf interne Bedrohungen der Demokratie zu reagieren, bedauerlicherweise schwach. Antidemokratische Tendenzen können sich wie Wundbrand ungehemmt in der gesamten EU ausbreiten, da Übertretungen durch nationale Regierungen straflos bleiben. Die EU ist schlecht gerüstet für die Abwehr solcher Angriffe auf die Demokratie von innen. Einerseits ist die EU sehr wohl eine politische Einheit, die supranationalen Gesetzen und supranationalen Institutionen unterliegt, mit einem Binnenmarkt, offenen Grenzen, Reisen ohne Pass, Unionsbürgerschaft und einem einheitlichen Raum der Sicherheit, Freiheit und Recht. Doch trotz feierlicher Bekenntnisse zu europäischen Werten werden diese Werte in der Praxis immer noch weitgehend als nationale Angelegenheit angesehen. Der Spähsoftware-Skandal deckt gnadenlos die Unreife und Schwäche der EU als *demokratische* Einheit auf. Was die demokratischen Werte anbelangt, stützt sich die EU auf die „Vermutung der Einhaltung“ durch die nationalen Regierungen, was sich aber in der Praxis zum „Anschein der Einhaltung“ entwickelt hat. Das Szenario, dass nationale Regierungen die EU-Rechtsvorschriften bewusst ignorieren und verletzen, ist in den EU-Governance-Strukturen schlicht nicht vorgesehen. Der EU wurden für solche Fälle keine Instrumente in die Hand gegeben. Die EU-Einrichtungen verfügen über wenig Befugnisse und noch weniger Lust, nationalen Behörden bei Übertretungen entgegenzutreten, und vor allem nicht im heiklen Bereich der „nationalen Sicherheit“. Nach zwischenstaatlicher Logik sind die Organe der EU den nationalen Regierungen untergeordnet. Ohne wirksame, sinnvolle supranationale Durchsetzungsmechanismen werden neue Rechtsvorschriften jedoch zwecklos sein. Die Lösung des Problems erfordert sowohl Regulierungsmaßnahmen als auch Governance-Reformen.

Auch die USA bleiben von Angriffen auf die Demokratie von innen nicht verschont, zum Beispiel Watergate oder die Besetzung des Kongresses am 6. Januar 2021, aber sie sind für energische Reaktionsmaßnahmen gerüstet. Sie haben die Befugnisse, selbst gegen die höchsten politischen Entscheidungsträger vorzugehen, wenn diese das Gesetz und die Verfassung nicht respektieren.

Nach den Enthüllungen über Spähsoftware im Jahr 2021 reagierten die Vereinigten Staaten rasch und entschlossen auf die Ergebnisse des Pegasus-Projekts. Das US-Handelsministerium setzte die NSO Group umgehend auf die schwarze Liste, das Justizministerium leitete eine Untersuchung ein, und eine strenge Regulierung für den Handel mit Spyware ist in Planung. Das FBI kam sogar nach Europa, um einen Spyware-Angriff gegen einen US- und EU-

Doppelstaatsbürger zu untersuchen. Tech-Giganten wie Apple und Microsoft haben juristische Beschwerden gegen Spyware-Unternehmen gestartet. Opfer haben Klage eingereicht, Staatsanwaltschaften ermitteln, und es wurden parlamentarische Untersuchungen eingeleitet.

Dagegen sind die anderen EU-Organe mit Ausnahme des Europäischen Parlaments weitgehend still und passiv geblieben und behaupten, dass es sich um eine ausschließlich nationale Angelegenheit handelt.

Der Europäische Rat und die nationalen Regierungen praktizieren Omertà. Es gibt keine offizielle Reaktion des Europäischen Rates auf den Skandal. Die Regierungen der Mitgliedstaaten haben die Einladung zur Zusammenarbeit mit dem PEGA-Ausschuss überwiegend abgelehnt. Einige Regierungen verweigerten strikt die Zusammenarbeit, andere waren freundlich und höflich, teilten aber aussagekräftige Informationen nicht wirklich. Selbst auf einen einfachen Fragebogen, der allen Mitgliedstaaten zu den Einzelheiten ihres nationalen Rechtsrahmens für die Verwendung von Spähsoftware übermittelt wurde, sind kaum substanzielle Antworten eingegangen. Buchstäblich am Vorabend der Veröffentlichung dieses Berichtsentwurfs erhielt der PEGA-Ausschuss über den Rat eine gemeinsame Antwort der Mitgliedstaaten, auch ohne wesentlichen Gehalt.

Die Kommission hat Bedenken geäußert und einige Regierungen der Mitgliedstaaten um Klarstellungen gebeten, aber nur zu den Fällen, die bereits einen Skandal auf nationaler Ebene ausgelöst hatten. Die Kommission gab – zögerlich und stückweise – Informationen über die Spyware-Angriffe an ihre eigenen Kommissionsbeamten weiter.

Europol hat es bisher abgelehnt, von seinen neuen Befugnissen zur Einleitung von Untersuchungen Gebrauch zu machen. Erst auf Drängen des Europäischen Parlaments richtete die Agentur ein Schreiben an fünf Mitgliedstaaten, in dem sie fragte, ob eine polizeiliche Untersuchung eingeleitet worden sei, und ihre Hilfe anbot.

Das Geschäft in Europa

Der Missbrauch von Spähsoftware wird meist durch die Brille der nationalen Politik betrachtet. Diese enge nationale Sicht verzerrt das Gesamtbild. Nur wenn alle Punkte miteinander verbunden werden, wird deutlich, dass die Angelegenheit in all ihren Aspekten zutiefst europäisch ist.

Auch wenn es keine offizielle Bestätigung gibt, können wir mit Sicherheit davon ausgehen, dass alle EU-Mitgliedstaaten ein oder mehrere kommerzielle Spyware-Produkte gekauft haben. Ein einziges Unternehmen, die NSO Group, hat seine Produkte an 22 Endnutzer in nicht weniger als vierzehn Mitgliedstaaten verkauft, darunter Polen, Ungarn, Spanien, die Niederlande und Belgien. In mindestens vier Mitgliedstaaten, nämlich Polen, Ungarn, Griechenland und Spanien, wurde Spähsoftware unrechtmäßig eingesetzt, und auch Zypern steht im Verdacht, sie zu verwenden. Zwei Mitgliedstaaten, Zypern und Bulgarien, fungieren als Drehkreuz für die Ausfuhr von Spähsoftware. Ein Mitgliedstaat, Irland, bietet einem großen Spähsoftware-Anbieter günstige steuerliche Regelungen, und ein anderer Mitgliedstaat, Luxemburg, dient vielen Akteuren der Spähsoftware-Branche als Drehscheibe für ihre Bankgeschäfte. Heimat der jährlich stattfindenden Europamesse der Spähsoftware-Industrie, der ISS World, auch als „Wiretappers Ball“ bezeichnet, ist Prag in der

Tschechischen Republik. Malta scheint ein beliebtes Ziel für manche Protagonisten der Branche zu sein. Hier ein paar beliebige Beispiele von Unternehmen, die „Europa ohne Grenzen“ für sich nutzen: Intellexa ist in Griechenland, Zypern, Irland, Frankreich und Ungarn präsent und sein CEO hat eine Reisepass- und (Briefkasten-)firma in Malta. NSO ist in Zypern und Bulgarien präsent und tätigt seine Finanzgeschäfte über Luxemburg. DSIRF verkauft seine Produkte aus Österreich, Tykelab aus Italien, FinFisher aus Deutschland (vor der Schließung).

Der Handel mit Spähsoftware profitiert vom EU-Binnenmarkt und dem freien Verkehr. Einige EU-Länder sind als Exportdrehscheibe attraktiv, da die Durchsetzung der Ausfuhrvorschriften – trotz des Rufs der EU als strenge Regulierungsinstanz – schwach ist. Als die Ausfuhrbestimmungen in Israel verschärft wurden, wurde die EU für Verkäufer attraktiver. Die Unternehmen werben für ihr Geschäft als „EU-reguliert“ und nutzen sozusagen ihre EU-Präsenz als Qualitätssiegel. „EU“ garantiert Seriosität. Die EU-Mitgliedschaft ist auch für Regierungen, die Spähsoftware kaufen möchten, von Vorteil: Die EU-Mitgliedstaaten sind von der einzelfallbezogenen Menschenrechtsbewertung, die für eine Ausfuhrlizenz der israelischen Behörden erforderlich ist, befreit, da die EU-Mitgliedschaft als ausreichende Garantie für die Einhaltung der höchsten Standards angesehen wird.

Auf der Verkaufsseite ist der Handel mit Spähsoftware undurchsichtig und schwer zu fassen, aber lukrativ und boomend. Die Unternehmensstrukturen sind praktischerweise, wenn nicht absichtlich, komplex angelegt, um unerwünschte Aktivitäten und Verbindungen – auch zu EU-Regierungen – vor den Augen zu verbergen. Auf dem Papier ist der Sektor reguliert, aber in der Praxis gelingt es ihm, viele Regeln zu umgehen, nicht zuletzt, weil Spähsoftware ein Produkt ist, das als politische Währung in internationalen Beziehungen dienen kann. Spähsoftware-Unternehmen sind in mehreren Ländern niedergelassen, aber viele wurden von ehemaligen israelischen Armee- und Geheimdienstoffizieren gegründet. Die meisten Anbieter behaupten, nur an staatliche Akteure zu verkaufen, obwohl einige im Hintergrund auch an nichtstaatliche Akteure verkaufen. Es ist praktisch unmöglich, Informationen über diese Kunden oder über die Vertragsbedingungen und Compliance zu erhalten.

Der Handel mit und die Verwendung von Spähsoftware fallen unmittelbar in den Anwendungsbereich des Unionsrechts und unter die EU-Rechtsprechung. Der Kauf und Verkauf von Spähsoftware unterliegt u. a. den Vorschriften für die Auftragsvergabe und den Ausfuhrregeln wie der Verordnung über Güter mit doppeltem Verwendungszweck. Die Verwendung von Spähsoftware muss den Standards der DSGVO, der EUDPR, der Richtlinie zum Datenschutz bei der Strafverfolgung und der Datenschutzrichtlinie für elektronische Kommunikation entsprechen. Die Rechte der Zielpersonen sind in der Charta der Grundrechte und in internationalen Übereinkommen, insbesondere das Recht auf Privatsphäre und das Recht auf ein faires Verfahren, sowie in den Unionsvorschriften über die Rechte von Verdächtigen und Beschuldigten verankert. Der Missbrauch von Spähsoftware stellt in vielen Fällen Cyberkriminalität dar und kann zu Straftaten der Korruption und Erpressung führen, die alle in den Zuständigkeitsbereich von Europol fallen. Wenn europäische Gelder im Spiel sind, hat der Europäische Staatsanwalt das Mandat zu handeln. Der Missbrauch von Spähsoftware kann auch die polizeiliche und justizielle Zusammenarbeit berühren, insbesondere den Austausch von Informationen und die Umsetzung des Europäischen Haftbefehls und der Beweisanordnung.

Der Missbrauch von Spähsoftware betrifft die EU und ihre Institutionen direkt und indirekt. Unter den Personen, die mit Spähsoftware ausspioniert wurden, waren Mitglieder des EU-Parlaments, der Kommission, des Rates und des Europäischen Rates. Andere waren als „Beifang“ betroffen und somit indirekte Ziele. Umgekehrt sitzen auch einige der „Täter“ im (Europäischen) Rat. Darüber hinaus wirkt sich die Manipulation der nationalen Wahlen unter Verwendung von Spähsoftware direkt auf die Zusammensetzung der EU-Organe und das politische Gleichgewicht in den EU-Governance-Gremien aus. Die vier oder fünf Regierungen, die beschuldigt werden, Spähsoftware missbräuchlich eingesetzt zu haben, machen fast ein Viertel der EU-Bevölkerung aus und haben somit im Rat erhebliches Gewicht.

Spähsoftware als Teil eines Systems

Spähsoftware ist kein bloßes technisches Werkzeug, das ad hoc und isoliert verwendet wird. Sie ist vielmehr integraler Bestandteil eines Systems. Im Prinzip ist ihre Verwendung in einen Rechtsrahmen eingebettet, der die erforderlichen Garantien, Aufsichts- und Kontrollmechanismen sowie Rechtsbehelfe vorsieht. Die Untersuchung zeigt jedoch, dass diese Schutzmaßnahmen oft schwach und unzureichend sind. Meist steckt keine Absicht dahinter, aber in einigen Fällen wurde das System – teilweise oder ganz – gezielt so hingebogen oder konzipiert, dass es als Werkzeug zur Ausübung politischer Macht und Kontrolle dient. In diesen Fällen ist die rechtswidrige Verwendung von Spähsoftware kein Zwischenfall, sondern Teil einer bewussten Strategie. Die Rechtsstaatlichkeit wird zum Gesetz des Herrschers. Die Rechtsgrundlage für die Überwachung kann so schwammig und ungenau formuliert werden, dass der breite und ungehinderte Einsatz von Spähsoftware legalisiert wird. Eine Ex-ante-Kontrolle in Form einer gerichtlichen Genehmigung der Überwachung kann leicht manipuliert und jeder Bedeutung entleert werden, insbesondere im Falle der Politisierung oder der Vereinnahmung des Justizwesens durch den Staat. Aufsichtsmechanismen können schwach und unwirksam gehalten und unter die Kontrolle der Regierungsparteien gebracht werden. Rechtsschutz und Bürgerrechte mögen auf dem Papier existieren, werden aber bei Behinderung durch staatliche Stellen hinfällig. Beschwerdeführern wird der Zugang zu Informationen verweigert, auch in Bezug auf die Vorwürfe, die gegen sie erhoben werden und ihre Überwachung angeblich rechtfertigten. Staatsanwälte, Richter und Polizei weigern sich zu untersuchen und wälzen oft die Beweislast auf die Opfer ab und verlangen von ihnen Beweise für den Angriff mit Spähsoftware. Für die Opfer bedeutet dies eine Catch-22-Situation, da ihnen der Zugang zu Informationen verweigert wird. Regierungsparteien können ihren Zugriff auf die öffentlichen Institutionen und Medien verschärfen, um eine sinnvolle Kontrolle zu untergraben. Der Regierung nahestehende öffentliche oder kommerzielle Medien können als Kanal für Verleumdungskampagnen mit dem durch Spähsoftware gewonnenen Material dienen. Häufig wird die „nationale Sicherheit“ als Vorwand für die Beseitigung von Transparenz und Rechenschaftspflicht angeführt. Alle diese Elemente bilden zusammen ein System, das auf Kontrolle und Unterdrückung ausgelegt ist. Dies führt nicht nur dazu, dass die einzelnen Opfer völlig schutz- und wehrlos gegenüber einer allmächtigen Regierung sind, sondern bedeutet auch, dass alle lebenswichtigen Kontrollen und Gleichgewichte einer demokratischen Gesellschaft außer Kraft gesetzt wurden.

Einige Regierungen sind bereits an diesem Punkt angekommen, andere befinden sich auf halbem Weg dorthin. Zum Glück werden die meisten europäischen Regierungen nicht diesen Weg einschlagen. Wenn sie es aber doch tun, ist die EU in ihrer derzeitigen institutionellen

und politischen Aufstellung nicht in der Lage, dies zu verhindern oder zu bekämpfen. Spähsoftware ist ein Frühwarnsignal: Sie deckt die gefährlichen konstitutionellen Mängel in der EU auf.

Geheimhaltung

Ein großes Hindernis bei der Erkennung und Untersuchung des rechtswidrigen Einsatzes von Spähsoftware ist die Geheimhaltung.

Für die meisten Opfer ist es nicht möglich, von den Behörden Informationen über ihren Fall zu erhalten. In vielen Fällen führen die Behörden Gründe der nationalen Sicherheit als Rechtfertigung für die Geheimhaltung an, in anderen Fällen leugnen sie schlicht die Existenz einer Akte oder die Akten werden vernichtet. Gleichzeitig weigern sich Staatsanwälte häufig, diese Fälle zu untersuchen, und argumentieren, dass die Opfer nicht über ausreichende Beweise verfügen. Dies ist ein Teufelskreis, der den Opfern keine Regressmöglichkeit lässt.

Regierungen weigern sich häufig, offenzulegen, ob und welche Art von Spähsoftware sie gekauft haben. Spähsoftware-Anbieter weigern sich ebenfalls, offenzulegen, wer ihre Kunden sind. Regierungen greifen für den Kauf von Spähsoftware oder damit verbundener Dienste oft auf Mittelsmänner, Vertreter oder persönliche Verbindungen zurück, um ihre Beteiligung zu verbergen. Sie umgehen die Vergabevorschriften und Haushaltsverfahren, um keine Spuren zu hinterlassen.

Israel ist eine wichtige Drehscheibe für Spähsoftware-Unternehmen und verantwortlich für die Erteilung von Vermarktungs- und Ausfuhrlizenzen. Obwohl Israel und Europa enge Verbündete sind, gibt Israel keine Informationen über die Erteilung (oder Aufhebung) von Lizenzen für die Ausfuhr von Spähsoftware in EU-Länder heraus, ungeachtet der Tatsache, dass diese verwendet wird, um die Rechte der europäischen Bürger zu verletzen und unsere Demokratie zu untergraben.

Anträge zur Informationsfreiheit von Journalisten liefern wenig bis gar keine Informationen. Auch die speziellen Kontroll- und Aufsichtsgremien wie die Datenschutzbehörden oder der Rechnungshof haben Schwierigkeiten, Informationen zu erhalten. Die unabhängige Aufsicht über Geheimdienste ist notorisch schwach und oft nicht existent. Parlamentarischen Untersuchungsausschüssen werden oft von den Regierungsparteien Steine in den Weg gelegt. Gerichtliche Untersuchungen konzentrieren sich auf Hacks durch Drittländer und nicht auf die rechtswidrige Nutzung durch EU-Regierungen. Journalisten, die über das Thema berichten, sind mit strategischen Klagen gegen die öffentliche Beteiligung (SLAPP-Klagen), verbalen Angriffen von Politikern oder Verleumdungskampagnen konfrontiert. Die mutigen und fleißigen Journalisten, die die Fakten des Skandals ans Licht bringen, verdienen unseren Respekt und unsere Dankbarkeit. Sie sind die Woodwards und Bernsteins Europas. Auch gibt es noch immer nicht in allen Mitgliedstaaten einen angemessenen Schutz von Hinweisgebern. In einigen Fällen sind es die Opfer eines Spyware-Angriffs selbst, die nicht aussagen wollen, um die hinter dem Angriff stehenden Parteien nicht zu entlarven, sei es aus Angst vor Vergeltungsmaßnahmen oder vor den Folgen, wenn kompromittierendes Material auftaucht.

Nächste Schritte

In einer Zeit, in der die europäischen Werte von einem externen Aggressor angegriffen werden, ist es umso wichtiger, unsere Demokratie und Rechtsstaatlichkeit gegen Angriffe von innen zu stärken. Die Feststellungen der PEGA-Untersuchung sind schockierend und sollten alle Bürgerinnen und Bürger in Europa alarmieren. Es ist offensichtlich, dass der Handel mit und die Verwendung von Spähsoftware streng reguliert werden sollten. Der PEGA-Ausschuss wird zu diesem Zweck eine Reihe von Empfehlungen abgeben. Es sollte jedoch auch Initiativen für institutionelle und politische Reformen geben, die es der EU ermöglichen, diese Regeln und Standards tatsächlich durchzusetzen und einzuhalten, selbst wenn es die Mitgliedstaaten selbst sind, die diese verletzen. Die EU muss ihre Verteidigungslinien gegen Angriffe auf die Demokratie von innen rasch weiterentwickeln.

ANGABEN ZUR ANNAHME IM FEDERFÜHRENDEN AUSSCHUSS

Datum der Annahme	8.5.2023
Ergebnis der Schlussabstimmung	+: 30 –: 3 0: 4
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Bartosz Arłukowicz, Vladimír Bilčík, Karolin Braunsberger-Reinhold, Saskia Bricmont, Anna Júlia Donáth, Cornelia Ernst, Giorgos Georgiou, Sylvie Guillaume, Hannes Heide, Ivo Hristov, Sophia in ‘t Veld, Assita Kanko, Beata Kempa, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Hannah Neumann, Carles Puigdemont i Casamajó, Diana Riba i Giner, Sándor Rónai, Ernő Schaller-Baross, Birgit Sippel, Dominik Tarczyński, Róża Thun und Hohenstein, Dragoş Tudorache, Lucia Vuolo, Jörgen Warborn, Juan Ignacio Zoido Álvarez
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Andrzej Halicki, Gabriel Mato, Thijs Reuten, Jordi Solé, Yana Toom
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter gemäß Artikel 209 Absatz 7	Aurélia Beigneux, Theresa Bielowski, Franc Bogovič, Catherine Griset, Andreas Schieder

NAMENTLICHE SCHLUSSABSTIMMUNG IM FEDERFÜHRENDEN AUSSCHUSS

30	+
PPE	Bartosz Arłukowicz, Vladimír Bilčík, Franc Bogovič, Karolin Braunsberger-Reinhold, Andrzej Halicki, Jeroen Lenaers, Gabriel Mato, Lucia Vuolo, Jörgen Warborn, Juan Ignacio Zoido Álvarez
Renew	Anna Júlia Donáth, Sophia in 't Veld, Moritz Körner, Róża Thun und Hohenstein, Yana Toom, Dragoş Tudorache
S&D	Theresa Bielowski, Sylvie Guillaume, Hannes Heide, Ivo Hristov, Juan Fernando López Aguilar, Thijs Reuten, Sándor Rónai, Andreas Schieder
Die Linke	Cornelia Ernst, Giorgos Georgiou
Verts/ALE	Saskia Bricmont, Hannah Neumann, Diana Riba i Giner, Jordi Solé

3	-
ECR	Beata Kempa, Dominik Tarczyński
NI	Ernő Schaller-Baross

4	0
ECR	Assita Kanko
ID	Aurélia Beigneux, Catherine Griset
NI	Carles Puigdemont i Casamajó

Erklärung der benutzten Zeichen:
+ : dafür
- : dagegen
0 : Enthaltung