**European Parliament**
2019-2024

*Plenary sitting*

**A9-0189/2023**

22.5.2023

# REPORT

of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware
(2022/2077(INI))

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

Rapporteur: Sophie in ‘t Veld

## CONTENTS

**Page**

DRAFT RESULTS ..... 3

EXPLANATORY STATEMENT ..... 140

INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE ..... 146

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE ..... 147

# DRAFT RESULTS

**of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI))**

*The European Parliament*,

– having regard to Article 226 of the Treaty on the Functioning of the European Union (TFEU),

– having regard to its decision of 10 March 2022 setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee,

– having regard to Rules 54 and 208 of its Rules of Procedure,

– having regard to the report of the Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware (A9-0189/2023).

***General introduction***

1. In July 2021, a collective of investigative journalists, NGOs and researchers – the Pegasus Project – published a report on the basis of a list in their possession of around 50 000 phone numbers that may have been targeted with Pegasus spyware. Such spyware has been widely used by both authoritarian and democratic governments around the world, both with and without judicial oversight, to target journalists, lawyers, judges, activists, politicians and state officials. People have been targeted with spyware in the European Union too: some by actors outside the EU, and others by actors within it, including government authorities. Most, if not all, Member State governments have bought spyware, in principle for law enforcement and security purposes. However, there is ample evidence that spyware has been abused in several Member States for purely political purposes, targeting critics and opponents of the parties in power, or in connection with corruption. Investigative findings link Pegasus and other surveillance spyware to various human rights violations by governments, including monitoring, blackmailing, smear campaigns, intimidation and harassment. This raises concerns at various levels of the EU legal order with respect to data protection and privacy, freedom of expression, freedom of the press, freedom of association, redress mechanisms, legal remedy and fair trial, and democratic processes and institutions. Although the use of spyware may pass the necessity and proportionality test in the event of serious threats to national security, the abuse of spyware for political purposes is extremely alarming and raises very serious concerns over the procedural and substantive lawfulness of surveillance practices and the level of protection granted by European and national law. Such abuse of spyware directly undermines fundamental rights and democracy, the core values on which the EU is founded. Subsequent investigative media reports and other sources have demonstrated that spyware is being exported from EU countries to third countries with undemocratic regimes and a high

risk of human rights violations, in blatant violation of EU export rules. The spyware industry is firmly established in the EU, benefiting from very favourable conditions for businesses.

2. In response to this growing scandal, on 10 March 2022 the European Parliament decided to set up a committee of inquiry pursuant to Article 226 TFEU in order to investigate alleged contraventions, or maladministration in the implementation, of Union law as regards the use of the Pegasus and equivalent surveillance spyware ('PEGA'). While a contravention constitutes the existence of illegal conduct, whether in the sense of actions or omissions in breach of the law, on the part of EU institutions or bodies or Member State authorities when implementing and enforcing EU law, maladministration means poor or absent administrative action, which occurs, for example, if the principles of good administration are not respected. Examples of maladministration include irregularities and omissions, abuse of power, unfairness, malfunction or incompetence, discrimination, but also avoidable delays, refusal to provide information, negligence and other shortcomings that imply poor application of Union law.

3. For the purposes of this inquiry, PEGA has used a broad approach as to what constitutes spyware, namely surveillance spyware that is installed on mobile devices by exploiting IT vulnerabilities. During the inquiry, the definition of 'cyber-surveillance items' laid down in the Dual-Use Regulation was also used: this definition describes them as 'dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems'. In September 2022, the Commission proposed a definition of spyware in its proposal for a Media Freedom Act, describing it as 'any product with digital elements that is specifically designed to exploit vulnerabilities in other products with digital elements and enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting or analysing data from such products or from the natural or legal persons using such products, in particular by secretly recording conversations or otherwise using the microphone of a terminal device, filming natural persons, machines or their surroundings, copying messages, taking photographs, tracking browsing activities, tracking geolocation, collecting other sensor data or tracking activities across multiple terminals, without the natural or legal person concerned being specifically informed and having given their explicit specific consent.'

4. On 19 April 2022, PEGA began its work, gathering information by means of public hearings, missions, consultation of experts, requests for data, evidence, and research.

5. During several public hearings, the inquiry investigated the functioning of spyware. Spyware is a type of malware that spies on a user's activities without their knowledge or consent. These spying activities can include keylogging, activity monitoring, and data collection, as well as other forms of data theft. Spyware is usually spread as a Trojan, or by exploiting software vulnerabilities[1]. Spyware can be installed remotely on the mobile phones of pre-identified individuals, even across borders. In some cases, telecom networks are used for the transmission of the spyware to the targeted device. Once the spyware has infiltrated the system, it disables protection mechanisms and security

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

updates. The infected device then transmits the collected data from the device and enables operators to conduct real-time surveillance by reading incoming text messages, tracking calls and locations and accessing and recording audio and video via the device's microphone and camera.

6. Contrary to conventional wiretapping, which only allows for the real-time monitoring of communications, spyware can provide full, retroactive access to files and messages created in the past, passwords, and metadata about past communications. As a result, a judicial decision on a start date and duration for a surveillance operation provides ineffective safeguards when spyware grants full retroactive access to data. It is also technically possible to impersonate the targeted person by gaining access to their digital credentials and identity. It is extremely difficult for the target to detect if there has been an intrusion with spyware. Spyware leaves few or no traces on the target's device, and even if it is detected, it is very difficult to prove who was responsible for the attack.

7. PEGA has received minimal or no answers from national authorities about the acquisition and use of spyware in their Member States, nor about the budgetary aspects. Vendors and countries issuing export licenses (mostly Israel) share no information about their customers. Many Member State authorities have not provided PEGA with meaningful information about the legal frameworks governing the use of spyware or about the use of spyware in their Member States beyond what was already publicly known, mainly due to national legal requirements relating to secrecy and confidentiality.

8. Some Member States have deployed spyware and refused to comment on it by invoking national security, which, according to Article 4(2) of the Treaty on European Union (TEU), 'remains the exclusive competence of each EU Member State'. However, case-law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) states that national security considerations have to be reconciled with the fundamental rights and democratic norms strongly embedded in EU law. Although it is for the Member States to define their essential national security interests and to adopt appropriate measures to ensure their internal and external security, the CJEU has held that 'the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law[2]', and it has clarified the criteria that Member States need to follow, when defining matters falling under national security. Several Member States have claimed that the use of spyware falls under national security and that this excludes the applicability of EU law. However, when Member States only provide a mere reference to national security as such, the restriction to fundamental rights cannot be justified as falling under national security. EU law must apply, with all the safeguards it provides. There is ample evidence of abuse of spyware for reasons wholly unrelated to national security. Member States should not be able to escape accountability for such grave spyware abuses, with a mere reference to national security. Because of this ambiguity, it was difficult to obtain sufficient information during hearings and missions and following information requests. The lack of clarity as to how national security is defined and the excessively broad

[2] Judgment of 6 October 2020, *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others*, C-623/17, EU:C:2020:790.

interpretation of its scope by the national authorities pose a challenge in understanding the justification for the use of spyware.

9. However, by putting together information from various sources, PEGA was able to reconstruct a partial but clear image, and could identify issues raising concern and meriting further investigation.

10. It can be safely assumed that authorities in all Member States use spyware in one way or another, some legitimate, some illegitimate. Spyware may be acquired directly, or through a proxy, broker company or middleman. There may also be arrangements for specific services, instead of actually purchasing the software. Additional services may be offered, such as training of staff or the provision of servers. Spyware is not to be seen in isolation, but as part of a wide range of products and services offered in an expanding and lucrative global market. It is important to realise that the purchase and use of spyware is very costly, running into millions of euros. But in many Member States this expenditure is not included in the regular budget, and it may thus escape scrutiny.

11. From information provided by the NSO Group, it is known that Pegasus was sold in at least 14 EU countries until the contracts with two countries were terminated. It is not know which countries these are, but there is a general assumption that they are Poland and Hungary. However, as long as the NSO Group or the Israeli Government does not make any official statement regarding a contract termination, this cannot be verified.

12. An additional piece of information is the attendee list of the 2013 ISS (Intelligence Support Systems) World fair, aka 'The Wiretappers Ball'. With the exception of Portugal and Luxembourg, all current EU Member States were represented by a wide range of organisations, including local police forces[3]. In recent years, the NSO Group has become the main sponsor of the event, but the sponsor list also includes Intellexa, Candiru, RCS and many others[4].

13. Member States are not just customers of commercial spyware vendors, they also have other, different roles in the spyware trade. Some host spyware vendors, some are the preferred destination for finance and banking services, and yet others offer citizenship and residency to protagonists of the industry.

14. In the vast majority of Member States, intelligence services are regulated by a legal framework – often with provisions on the organisation and functioning of these services as well as their mandates and powers, including their means of action and conditions for using them – and oversight mechanisms that include executive control, parliamentary oversight, expert bodies, and judicial review. Yet concerns have been raised about certain countries' permissive intelligence frameworks, ineffective checks, lax oversight practices and political interference**.**

15. Spyware is clearly also used by law enforcement, not just by intelligence agencies. There are serious concerns about the admissibility in court of such material as evidence in the context of EU police and justice cooperation, including within Europol and Eurojust, if such information were to originate from investigation methods applied

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

without proper judicial oversight. Depending on the national legislation, the use of spyware is legitimate in investigations under judicial oversight.

16. The abuse of spyware is a threat to democracy and fundamental rights. Since the revelations of the Pegasus Project, the United States have taken several steps to investigate and regulate it. Within the EU there has been very little action so far. Clear rules must be laid down on the use of, and trade in, spyware, preferably in tandem with other countries, such as the US.

## *I. The use of spyware in the EU*

### *I.A Poland*

17. The representatives of the ministries declined to meet the delegation of the committee. In response to the questionnaire sent out by PEGA on 15 July 2022, the Polish authorities did not answer all of the questions and insisted that the existing provisions were sufficient, and that they were operating strictly within the law[5]. The Minister of the Interior, Mariusz Kaminski, also refused to accept an invitation by PEGA to exchange views[6].

18. PEGA's fact-finding mission to Poland in September 2022 was of paramount importance for the committee, allowing it to gather information and facts on the use of Pegasus spyware. The meetings held in Warsaw shed new light on the illegal use of intrusive surveillance software against democratic actors in Poland. Members learned how the system of legal and institutional checks and balances has been dismantled to enable the targeting of individuals deemed to be political opponents with military-grade cyber weapons. As a result, crucial democratic standards and citizens' rights enshrined in EU and Polish laws have been grossly violated. This is yet another dimension of the crisis of the rule of law in Poland.

#### PURCHASE OF PEGASUS

19. In November 2016, former Prime Minister and current MEP Beata Szydło and former Foreign Minister Witold Waszczykowski attended dinner at the home of then Prime Minister of Israel Benjamin Netanyahu[7]. The following year in July, Szydło and Netanyahu met with the heads of governments of the Visegrad Group countries. They allegedly discussed 'strengthening cooperation in the area of innovation and high technologies' and 'issues related to the broadly understood security of citizens'[8]. Not long after this meeting took place in 2017, Pegasus was acquired by the Polish Government following a meeting between Prime Minister Mateusz Morawiecki, Hungarian Prime Minister Viktor Orbán and Netanyahu[9]

---

[5] Response by the Permanent Representative of Poland to the EU, Andrzej Sadós, to the PEGA Committee, 7 September 2022.
[6] Response by Minister of the Interior, Mariusz Kaminski, by letter to the PEGA Committee, 12 July 2022.
[7] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29 January 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.

20. Initially, the Polish Government and PiS leader Jarosław Kaczyński denied the purchase of Pegasus[10]. However, in early January 2022, they confirmed the purchase of spyware by the Polish Government[11] [12] [13]. In the same month, it was revealed that key evidence related to the purchase of Pegasus had been collected by the Supreme Audit Office in 2018 during an audit of the Justice Fund operated by the Ministry of Justice and set up to support victims of crime. On 18 January 2022, former Chief of the Polish Supreme Audit Office (NIK) and subsequently independent Senator Krzysztof Kwiatkowski testified on the purchase of Pegasus before the Senate Extraordinary Committee on Cases of Surveillance Using the Pegasus System[14]. Having been released from the secrecy requirement associated with his position, he presented two invoices to the committee confirming the purchase of spyware for the Central Anti-Corruption Bureau (CBA), with PLN 25 million from the Justice Fund run by the Ministry of Justice[15]. Kwiatkowski testified that the NIK had discovered accounts from the National Bank of Poland certifying the transfer[16].

21. The invoices were issued by Matic Sp. z o.o., which acted as an intermediary through which the CBA carried out this purchase[17]. Matic Sp. z o.o. is an IT and security company based in Warsaw, owned and run by persons active in the intelligence and security services community during the communist period[18].

22. Matic became a joint-stock company immediately after the purchase of Pegasus in November 2017 and operates with a licence from the Ministry of Internal Affairs for trading in technologies with the security services and police, and in the arms trade according to Wyborcza[19].The company is also in possession of a special licensing certificate from the Internal Security Agency, with the most recent one issued in 2019, that will allow it to keep certain confidential information secret until the end of the decade[20]. Representatives of Matic declined to meet and share information with the committee of inquiry.

23. According to Polish law, the operations of the CBA can only be financed from the state budget. However, the purchase of Pegasus was financed through the Justice Fund,

---

[10] https://www.politico.eu/article/poland-government-scrambles-minimize-hacking-backlash/.
[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.

which is not part of the state budget but a public fund earmarked for victims of crime[21]. The purchase therefore breached Polish law. Moreover, the original regulations governing this fund do not allow it to be used to finance operations of the special services[22]. However, in September 2017, a motion to change the financial plan of the Justice Fund was presented to the Sejm (lower house of the Polish Parliament) Public Finance Committee by Michał Woś, the Deputy Minister of Justice[23] and a close associate of the Minister of Justice, Zbigniew Ziobro[24]. The MPs approved this change. When it was later revealed that the Justice Fund was used to finance Pegasus for the CBA, MPs said that 'during the committee meeting, not a single word was said about it'[25]. It therefore appears that they were misled by the government. Although the NIK has submitted an official notification to the Prosecutor's Office regarding a violation of the law concerning the use of resources from the Justice Fund to purchase Pegasus in 2017, there is no expectation that the Prosecutor's Office will take action on such a case, given the current institutional and political environment.

24. Woś also applied to the Ministry of Finance for consent to reallocate the PLN 25 million that was spent on Pegasus from the Justice Fund to 'other activities' aimed at 'combating the effects of crime'. The Deputy Minister then gave approval to the transfers from the Justice Fund to the CBA. However, upon being asked in January 2022, Woś initially denied having any knowledge of the Pegasus tool itself, let alone its purchase by the state, but he has since confirmed the purchase. It is unclear how the running costs for the use of Pegasus have been funded.

25. It has been reported that in total, the NSO Group has sold Pegasus to 14 countries in Europe thus far. However, the NSO Group has also conceded that it has revoked the licences of two such countries[26]. During its testimony in the PEGA Committee, the NSO Group stated that it only investigates 'issues' regarding the use of Pegasus when it receives information from whistleblowers or through the media. When the NSO Group receives complaints, it investigates and reviews them, and subsequently it can shut down Pegasus for actors who have misused it[27]. Based on the large number of media reports on the use of Pegasus in Poland, it is highly likely that Poland was included as one of these two countries in the light of their breach of the NSO terms of use; however,

---

[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; 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. 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] Discussion with NSO Group, Mission of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware to Israel, July 2022.

[27] Testimony by Chaim Gelfand, General Counsel and Chief Compliance Officer, NSO, in PEGA, 21 June 2022.

this has not been confirmed.

26. Since the first signs of use of Pegasus by the Polish authorities, the Polish Ombudsman has been attempting to inquire with the authorities whether this was the case and has argued for the improvement of democratic and human rights safeguards to prevent the abuse of surveillance, including through yearly reports to the Polish Parliament. In January 2023, the Polish Ombudsman sent a letter to the Minister of Internal Affairs stating that there was no legal basis for the use of Pegasus or similar spyware in Poland, invoking the case-law from the Polish Constitutional Court as well as case-law from the ECtHR[28].

LEGAL FRAMEWORK

27. In 2014, the Constitutional Tribunal conducted a review of the 1990 Police Act and other existing laws governing the surveillance of citizens that were deemed incompatible with the Constitution of Poland[29]. The Tribunal concluded by issuing a judgment containing specific recommendations and an 18-month timeline within which legislative changes were to be implemented[30]. Following the 2015 elections, the new government introduced legislative changes. However, the resulting Act of 15 January 2016 amending the 1990 Police Act and Certain Other Acts (hereinafter the 2016 Police Act) did not rectify any of the gaps in the law, as was required by the Constitutional Court[31]. Instead, the 2016 Police Act has weakened the existing provisions, which in themselves neither sufficiently protected the rights of citizens nor created proper oversight.

28. In its opinion on the 2016 Police Act, the Venice Commission states that '... procedural safeguards and material conditions set in the Police Act for implementing secret surveillance are still insufficient to prevent its excessive use and unjustified interference with the privacy of individuals'[32]. Moreover, the lack of specificity regarding oversight, guarantees against abuse and the categories of persons and crimes that could be targeted also violates ECtHR judgments[33]. In particular, in the judgment on the *Roman Zakharov* v. *Russia* case in 2015, the court examined the need for clarity regarding the use of spyware. It was held that in relation to the secret surveillance of citizens there is a necessity for strict criteria, proper judicial oversight, the immediate destruction of irrelevant data, judicial scrutiny over urgency procedures and a requirement for the notification of victims[34]. Moreover, the court explicitly stated that it would be 'contrary to the rule of law' if discretion regarding secret surveillance was concentrated entirely

[28] PEGA Committee meeting, 19 January 2023.
[29] Opinion No. 839/2016 on the Act of 15 January 2016 amending the Police Act and certain other acts, adopted by the Venice Commission at its 107th plenary session, 10-11 June 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] Opinion No. 839/2016 on the Act of 15 January 2016 amending the Police Act and certain other acts, adopted by the Venice Commission at its 107th plenary session, 10-11 June 2016.
[33] See, inter alia, *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.

with the executive of the judiciary[35]. The 2016 Police Act that remains in effect in Poland in no way reflects this ruling of the court. In fact, its provisions are in direct contravention of much of the judgment.

29. The ECtHR has also been unequivocal in its stance on the necessity test, meaning that the act of surveillance must be of sufficient importance to necessitate such an invasion of privacy. Its judgment in the *Klass and others* v *Germany* case in 1978 outlined this point clearly, and held that no matter the system of surveillance, the court must be satisfied that 'adequate and effective guarantees against abuse'[36] exist. The carefully orchestrated destruction of checks and balances in Poland shows the evident defiance of the courts by the ruling party. Despite all of this, the PiS-led government insists that the existing provisions are sufficient, and they are operating strictly within the law[37]. At the same time, the government has declined all requests for dialogue and clarification about how surveillance is used in Poland.

*2016 ANTI-TERRORISM ACT*

30. In addition to the 2016 Police Act, in 2016 the Sejm adopted a law governing the surveillance of foreign citizens that it dubs the 'Anti-Terrorism Act'. The act stipulates that non-Polish citizens can be monitored without the court's consent for a period of three months if their identity is 'doubtful', including through the wire-tapping of phones, the collection of fingerprints, biometric photos and DNA, and the obligation to register pre-paid phone cards[38]. According to the Article 9.8. of the act, the Prosecutor-General has the power to order the destruction of non-relevant materials. Given the fact that the current Prosecutor-General, Zbigniew Ziobro, is also the Minister of Justice, there are serious concerns as to whether he is capable of taking independent and impartial decisions without being influenced by the political interests of the government he represents[39] [40].

*CODE OF CRIMINAL PROCEDURE*

31. In July 2015, the Act Amending the Code of Criminal Procedure was introduced in Poland to ensure that illegally obtained evidence could not be included in criminal proceedings. However, after PiS came to power, the act was revised in March 2016 in order to include Article 168a[41]. This addition ensures that evidence gathered in violation of the law, or 'fruit of the poisonous tree', such as information harvested through the

[35] *Roman Zakharov* v. *Russia* [GC], no. 47143/06, ECtHR, judgment of 4 December 2015, paragraphs 229 and 230. See also Opinion No. 839/2016 of the Venice Commission, June 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e, p. 11.
[36] *Klass and others* v. *Germany*, 6 September 1978, paragraph 50, Series A no. 28. 40.
[37] Letter from Mariusz Kaminski, Minister of the Interior and Administration of Poland, to the PEGA Committee, 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.
[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.

use of Pegasus, is eligible to be used in criminal proceedings[42]. However, it must be added that the Supreme Court of Poland indicated in a judgment that this article cannot be applied in contradiction of the provisions of the European Convention on Human Rights and the Constitution of Poland, which in some cases limits its effective application[43]. Judgments have also been issued in which Article 168a has been found partially unconstitutional[44]. Nevertheless, the presence of this provision in the legal system raises uncertainty when it comes to respect for fundamental rights.

*TELECOMMUNICATIONS LAW*

32. After the 2016 amendment to the Telecommunications Act of 2004, the law governing telecommunications in Poland includes provisions allowing the police to gain unrestricted access to metadata and in certain cases, to do so without the involvement of the telecommunication companies[45]. Such access can be obtained under a very broad justification of 'prevention or detection of crimes'. The prosecutor then decides how to proceed upon receipt of this data. This cannot be regarded as a safeguard, however, given the fact that through the merging of the role of Minister of Justice and that of Prosecutor-General, the prosecution service cannot be considered as independent from the executive[46].

33. The abovementioned amendment to the Code of Criminal Procedure to allow 'fruit of the poisonous tree' has had a significant impact on the importance of telecommunications operators and the data these companies store. In Poland, the biggest telecommunications providers are effectively obliged to have a dedicated team that responds to multiple wiretapping requests from the authorities. However, they usually do not have much insight into the content of wiretapping or operational details of individual cases[47].

*THE ACT IMPLEMENTING THE LAW ENFORCEMENT DIRECTIVE*

34. Poland has not properly implemented the Law Enforcement Directive (EU) 2016/680[48], which requires specific standards for the collection and processing of personal data by the police and other services. The Law Enforcement Directive was transposed into

---

[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] For example, the judgment of the Supreme Court of Poland of 26 June 2019, IV KK 328/18.
[44] For example, the judgment of the Supreme Court of Poland of 26 June 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.
[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 February 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, pp. 16-17.
[48] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

Polish law by the 2018 Act on the protection of personal data processed in connection with the prevention and combating of crime. The act has significantly extended the scope of the grounds provided for in the directive for refusing to notify individuals of the processing of their data and has disregarded the mechanism provided for in Article 17 of the directive, giving individuals the opportunity to exercise their power through the relevant supervisory authority – in Poland, the President of the Office for Personal Data Protection. Furthermore, the act provides for a significant carve-out for national security, including the implementation of statutory tasks by various agencies of the security forces[49].

35. Poland has also not yet implemented the EU Whistleblowers Directive. It did not meet the December 2021 deadline after its initial draft legislation failed. A second draft was published in April 2022 but there has been no further progress and the proposed legislation contains significantly weaker provisions. In January 2022, the Commission opened an infringement procedure against Poland for failing to fully implement the directive, and in February 2023, the Commission decided to refer Poland to the CJEU[50].

36. The Sejm, in particular members of PiS, are currently drafting an electronic communications law. This law would make it easier for the authorities to access the emails and social media messages of Polish citizens. Providers would have to store emails and messages on their servers so that relevant courts could issue orders to access the data, IP addresses and the content of the messages[51].

*EX ANTE* SCRUTINY

37. Although, as a rule, surveillance in Poland requires judicial authorisation, the existing authorisation procedure does not serve as a safeguard against abuse, but rather as a mean to grant a veneer of legality to surveillance for political purposes. It has not been made explicitly clear whether any of the persons targeted by Pegasus to date were spied on with judicial authorisation. Applications for judicial authorisation of a surveillance operation are submitted by the special services[52]. For the assessment of the application, judges only have the information provided by the applicant (i.e. the special services) at their disposal, and it is the prosecutor who decides what material is relevant to be submitted[53]. The information is often merely a summary, sometimes excluding even the most basic details regarding the targeted person (name, profession, the crime of which they are suspected) and a description of the surveillance methods to be used.

38. If a judge rejects an application, they are required to give a reasoned justification for

[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/en/ip_23_703.
[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 .

such a decision and it can be subject to appeal[54]. In urgent cases, the prosecutor can initially authorise the use of interception methods without the approval of a judge, provided the court subsequently grants authorisation within five days[55]. This is a significant and deliberate loophole in the Polish legal framework.

39. Requests for the authorisation of surveillance by the main agencies, i.e. the CBA, the police (Policja KGP) and the intelligence services (Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, Służba Ochrony Państwa, Biuro Nadzoru Wewnętrznego MSWiA, and the recently added Inspektorat Służby Więziennej) are submitted almost exclusively to the District Court in Warsaw (Sad Okręgowy), where most of these agencies are located.

40. Several dozen surveillance applications are submitted every day, stretching the capacity of the court to conduct an in-depth examination of each request[56]. The system which randomly allocates cases to the judges of the courts is technically still in operation in Poland, but it is only functional during business hours. However, given that the court which authorises surveillance functions on a 24-hour basis, there is ample opportunity for the system to be circumvented. By submitting an application at the weekend or outside normal business hours, the case will be automatically assigned to the judge who is on call[57]. The information regarding who is on call at any given time is known to the secret services, who are then essentially able to select a 'friendly judge' to whom they can submit their surveillance requests[58]. Moreover, random allocation can also be bypassed by IT personnel who have access to the system and are able to assign surveillance authorisations to 'friendly judges'[59]. All this severely undermines the capacity of the court to perform effective judicial oversight.

*EX POST* SCRUTINY

41. Parliamentary oversight is virtually non-existent in Poland. Before 2016,the Parliamentary Oversight Committee for the Special Services (KSS) was led by rotating the chair between the ruling and opposition parties. However, PiS has changed this parliamentary rule and installed PiS members Waldemar Andzel as permanent Chair and Jarosław Krajewski as Deputy Chair of this committee[60]. The government parties have the absolute majority in the committee[61]. This renders the oversight function of the committee meaningless. Moreover, the government majority in the Sejm rejected calls for a parliamentary investigation into the allegations of the illegitimate use of spyware[62]

[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] Testimony of Ewa Wrzosek, country-specific hearing on Poland, meeting of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware on Poland, 15 September 2022.
[57] Testimony of Ewa Wrzosek, country-specific hearing on Poland, meeting of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware on Poland, 15 September 2022.
[58] Testimony of Ewa Wrzosek, country-specific hearing on Poland, meeting of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware on Poland, 15 September 2022.
[59] Testimony of Ewa Wrzosek, country-specific hearing on Poland, meeting of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware on Poland, 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 January 2022.

[63] [64] [65] [66]. On the other hand, the Senate, where the government parties hold no majority, set up an inquiry committee in early 2022. However, the Senate committee lacks the investigative powers of the Sejm[67], whose inquiry committee can summon witnesses and hear sworn testimony. The committee has been opposed at every turn by the ruling party in the Sejm[68], government officials and security agencies, all of which have refused to cooperate or conduct their own investigation[69].

42. The scrutiny and remedies offered by other independent bodies have also been severely weakened. The Supreme Audit Office has effective powers of oversight; however, its members and staff are subject to constant obstruction, harassment and intimidation, which is severely affecting its operational capacity[70]. The Sejm has so far failed to appoint 10 of the 19 members of the NIK Council[71].The required vetting of council members carried out by the special services, headed by Minister Kaminski, is very slow[72].

43. When a violation of the law is discovered by the NIK, they have the power to submit a notification to the Prosecutor's Office[73]. However, it is up to the Office of the Prosecutor to initiate a case on the basis of that notification. In situations where the Prosecutor does not take action, there is little that can be done by the NIK. When a reported violation concerns the operations of the Prosecutor's Office itself, a vicious circle of non-accountability is created. In addition, all cases notified by the NIK to the Prosecutor's Office must be reported to the Prosecutor-General, who is also the Minister of Justice, heading the very ministry that purchased the spyware in the first place. The Prosecutor-General has the power to discontinue investigations or resume investigations

[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 December 2021.
[65] The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', 24 January 2022.
[66] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/ , 18 January 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, footnote 220.
[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 January 2022.
[69] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17 January 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 December 2021; The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', 24 January 2022; Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 January 2022.
[70] Reuters, https://www.reuters.com/article/poland-pegasus-idUSL8N2UF596, 4 February 2022; discussion with Supreme Audit Office, mission of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware to Poland, September 2022.
[71] https://www.nik.gov.pl/en/about-us/the-council-of-nik/; discussion with Supreme Audit Office staff, mission of the Committee of Inquiry to Investigate the use of Pegasus and equivalent surveillance spyware to Poland, September 2022.
[72] Discussion with Supreme Audit Office staff, mission of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware to Poland, 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.

that had been terminated by the prosecution service. He can also initiate disciplinary proceedings against prosecutors whom he suspects of having taken wrong decisions.

44. The current Ombudsman, Marcin Wiącek, was appointed in 2021 when the Sejm and the Senate agreed on a non-partisan compromise candidate after a long tug of war[74]. Regarding the case of Senator Brejza, Wiącek argued that the Ombudsman should not get involved in the early stages of a case. In spite of this, both the former and current Ombudsmen have been monitoring the situation and exerting a certain amount of pressure concerning the need to create an independent oversight body to provide democratic scrutiny over the operations of the secret services[75].

REPORTING

45. Under the 2016 Police Act, the police are only required to submit reports twice a year to the competent courts regarding the number of collections of telecommunication, postal or internet data along with their legal reasoning (relating to prevention or detection of crimes, the protection of human life or health or supporting search and rescue operations)[76]. These reports can only be produced *ex post* and are not made public. If there is an issue with the submission, the court will submit its findings in response within 30 days but cannot order the destruction of any data, even if it finds incompatibilities with the law. Most importantly, these supervisory actions are only optional, not mandatory.

REDRESS

46. So far, despite the ample evidence that serious crimes have been committed, the Polish Prosecutor has been acting in a very dilatory manner. It seems that only the case of prosecutor Ewa Wrzosek and Krzysztof Brejza have been taken up by the courts. Wrzosek initially filed her case with the Prosecutor's Office. However, upon its official refusal to take up the case, she was able to appeal to the courts. In late September 2022, the Warsaw District Court (Mokotów) ordered the Prosecutor to begin an investigation. So far, however, the Prosecutor has failed to undertake any meaningful proceedings that are necessary for the cases to progress, such as gathering testimony from the targeted person.

47. It is critical to note that Wrzosek was only able to initiate this appeal in the courts as a result of obtaining an official refusal from the Prosecutor's Office. In many other instances, the Prosecutor drags out the investigation in order to avoid ever having to issue an official response, as he is aware that if he does so, he will be exposed to the appeals process in the courts.

48. Citizens who have been targeted can bring a civil case before court, but the burden of

[74] Euractiv, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/, 22 July 2021.

[75] European Parliament. Directorate-General for Parliamentary Research Services, 'Europe's PegasusGate: Countering spyware abuse', study , 6 July 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 .

proof that they were the subject of surveillance is on them and it is virtually impossible to prove the illegitimate use of spyware without the cooperation of the authorities. The lack of implementation of the duty to notify in Poland, as outlined in the *Klass* judgment, means that many persons may never know they have been targeted.

49. Currently, the cases *Pietrzak* v *Poland* and *Bychawska-Siniarska and others* v *Poland* are before the ECtHR, challenging the lack of transparency, oversight, notification and remedies when it comes to surveillance in Poland. Significantly, the court decided to conduct a rare hearing for these cases, which took place on 27 September 2022. The cases were taken by five citizens[77] who submitted complaints to the ECtHR in September 2017 and February 2018 respectively. Eleven entities submitted *amicus curiae* briefs in this case, including the European Criminal Bar Association[78], the Polish Ombudsman, and the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism[79].

50. Although this avenue of complaint before the ECtHR is open to citizens, it is questionable as to whether this qualifies as an effective legal remedy, given the length of the proceedings. Five years after the initial complaint, there is still no court decision in this case.

51. On the basis of Article 227 of the Code of Administrative Procedure, complaints had been submitted earlier in 2017 to the Prime Minister and the respective heads of the various police and intelligence services. These intelligence services included the CBA, the Internal Security Agency, the National Tax Administration, the Military Counterintelligence Service, the national police, the border police and the national gendarmerie. Their complaints pertained to the fact that the legislation permitted members of these police and intelligence services to monitor their telecommunications and digital communications without their knowledge. As the members of the services in question were not required to inform them about possible surveillance, the applicants were consequently unable to have the lawfulness of that activity reviewed by a court, which, in their view, was contrary to the Polish Constitution.

52. Between June and September 2017, the heads of the abovementioned police and intelligence services sent their responses to the applicants' complaints. Relying on Article 8 (right to respect for private and family life) of the European Convention on Human Rights, the applicants complained that the secret systems for monitoring telecommunications, postal and digital communications and gathering metadata, introduced in application of the Police Act, and the Anti-Terrorism Act, interfere with their right to respect for their private life. Relying on Article 8, taken together with Article 13 (right to an effective remedy), the applicants allege that they had no effective remedy which would have enabled them to establish whether they themselves had been

[77] Mikołaj Pietrzak, lawyer, Dean of the Warsaw Bar; Dominika Bychawska-Siniarska, member and employee of the Helsinki Foundation for Human Rights; Barbara Grabowska-Moroz, university lecturer and researcher and external expert of the Helsinki Foundation for Human Rights; Wojciech Klicki and Katarzyna Szymielewicz, members of the Panoptykon Foundation based in Warsaw.

[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.

subjected to secret surveillance and, if necessary, to have the lawfulness of that surveillance reviewed by a court.

PUBLIC SCRUTINY

53. The independent media are another element of democratic checks and balances, exercising public scrutiny. However, in the case of the use of spyware, the Polish public broadcaster, which is largely controlled by the government parties, actually became complicit in the illegitimate surveillance scandal by making public materials obtained from the smartphones of several of the targeted persons, including the opposition Senator Krzysztof Brejza. Making public information obtained in a special services surveillance operation is a criminal act in itself, yet, no action has been taken by the police or the public prosecutor.

POLITICAL CONTROL

54. Many key positions throughout the entire chain are held by members or loyalists of the government parties. Minister of the Interior and Coordinator of the Special Services Kaminski was convicted in 2015 of abuse of power and sentenced to three years' imprisonment[80]. However, immediately after the 2015 parliamentary elections President Duda pardoned him in a highly irregular manner, which was condemned by among others, the Polish Supreme Court, the CJEU, the Venice Commission and the US Department of State. This raises concerns about his independence and neutrality. Kaminski has declined to meet or cooperate substantially with the PEGA Committee[81].

55. The CBA is fully controlled by the ruling majority and lacks independence, despite its title and its mandate, which was established under the Act of 9 June 2006 on the Central Anti-Corruption Bureau[82], Article 1.1 of which states that '[t]he Central Anti-Corruption Bureau ... is established as a special service to combat corruption in public and economic life, particularly in public and local government institutions as well as to fight against activities detrimental to the economic interest of the State'[83]. In the 2022 Annual Rule of Law Report, the Commission finds that '[t]he independence of main anti-corruption institutions remains an issue, considering in particular the subordination of the Central Anti-Corruption Bureau to the executive and the Minister of Justice also being the Prosecutor-General'[84].

56. The government's efforts to gain control over the judiciary have been widely documented and confirmed by a wide range of instances, including the Commission, the CJEU and the ECtHR.

57. Not only has the legal and institutional context been created to enable near unlimited

[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, Article 1.1.
[84] 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. 1.

surveillance with spyware, but virtually all parts of the process are also firmly controlled by the government parties. As a result, safeguards that may exist on paper have zero or little meaning in practice.

THE TARGETS

58. The first documented cases of the use of Pegasus in Poland date back to 2018. One of these concerned the former Deputy Minister of the Treasury, Paweł Tamborski, whose phone was hacked with Pegasus in February 2018, as revealed by Amnesty International and Wyborcza in July 2022. On the same day, the CBA detained him and five former officials of the ministry and market analysts, who were accused of underestimating the market value of the CIECH chemicals company in exchange for bribes. The court did not agree with the arrest and ordered their release. The CEO and owner of Cross Media PR agency, Andrzej Długosz, was also targeted, and ended up being hacked at least 61 times between March 2018 and November 2019. Subsequently, the Ombudsman requested more information from the authorities, but the effort was in vain. At that time, the government continued to deny having purchased the spyware.

59. Following the investigations of the Associated Press and the Citizen Lab researchers at the University of Toronto, it was revealed that three more persons had been targeted with Pegasus in Poland in 2019[85], namely the opposition Senator, Krzysztof Brejza, the lawyer, Roman Giertych, and the prosecutor, Ewa Wrzosek. While some members of the ruling majority have confirmed the purchase of the software from the NSO Group, the government has not officially acknowledged that any specific persons were targeted. None of the three targets, have been formally charged with any crime, nor have they been summoned for questioning, nor has there been a request to lift the immunity of the targets who hold public office in connection with this case.

60. Citizen Lab had detected a number of infections in Poland in late 2017; however, they were not able to identify the targeted persons at that time[86].

61. The use of spyware and efforts to control citizens must be viewed in close connection with the electoral system. Several targets of Pegasus were connected to elections in some capacity: Senator Krzysztof Brejza (head of the election campaign of the largest opposition party), Roman Giertych (lawyer of the opposition leader and former President of the European Council, Donald Tusk), Ewa Wrzosek (the prosecutor investigating postal voting for the presidential elections), the Supreme Audit Office (NIK) (which published reports on the postal vote for the presidential elections) and Michael Kolodziejczak (founder of an agrarian political party that competes for the same electorate as the government parties).

62. At the same time, the independence of the National Electoral Commission has been called into question by virtue of the fact that it is comprised of judges selected by the Parliament and courts that the ruling party has brought under its control. Furthermore,

[85] The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware , *17 February 2022.*
[86] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.

the District Court in Warsaw responsible for the registration of new political parties[87] has been filled with government-loyal 'neo-judges', whose independence could be called into question.

*KRZYSZTOF BREJZA*

63. Senator Krzysztof Brejza was serving as the head of the election campaign of the opposition party Civic Platform during the European and national elections when he became the target of hacking with spyware[88]. There were 33 attacks on Brejza's phone while he was running the Civic Platform's parliamentary election campaign in 2019, with the attacks beginning on 26 April 2019 and continuing until 23 October 2019, just days after the end of the election cycle[89].

64. As a direct result of the hacking of Brejza's phone, text messages were allegedly stolen, doctored and subsequently aired on the state-controlled television network (TVP)[90] during the 2019 elections in an alleged orchestrated smear campaign[91]. This has caused Senator Brejza to call into question the legitimacy of the 2019 election, which was narrowly won by the ruling PiS party[92].

65. Although the PiS government admits to obtaining Pegasus, it vehemently denies allegations that it was used for political purposes[93]. Kaczynski has neither confirmed nor denied targeting Brejza, but has alleged that the senator was linked to 'suspected crimes', something Brejza strongly denies[94]. No charges were ever brought against Brejza and he was never summoned to testify. This indicates that the use of spyware did not serve any investigative purpose. Through the implication that Brejza was linked to criminal activity, the government attempted to formally legitimise the use of spyware by creating circumstances through which the Polish Government could use the Pegasus spyware for one of the grounds that the NSO Group deems 'legitimate' when considering whether to sell their software to a government, namely the investigation of serious criminal activity[95].

66. For weeks on end, Senator Brejza was the target of a smear campaign that made use of material obtained through the use of the Pegasus spyware. It is remarkable that such

[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] 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.
[91] 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.
[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.

material was made public via public television. No explanation can be given for how a public broadcaster obtains access to such material. If the Pegasus hack of Senator Brejza had indeed been a matter of national security, as the government seems to suggest, it would be a very serious crime to leak the material obtained in a secret security operation. The fact that the public broadcaster has also been captured by the government party points instead in the direction of a smear campaign orchestrated by the government parties.

67. At the time, however, a criminal investigation into Senator Brejza's father, Ryszard Brejza, was initiated. While serving as the mayor of Inowroclaw, a city in central Poland, Brejza Sr was called in for questioning in relation to alleged mishandling of public funds and failing to carry out his duties[96]. This questioning occurred directly after Brejza Jr initiated legal proceedings against Kaczynski for slander. Both Krzysztof and Ryszard Brejza have asserted that the charges against Brejza Sr were in retaliation for the lawsuit.

68. Ryszard Brejza himself received 10 text messages between July and August 2019 which Amnesty International's security lab deemed suspicious and which matched the hallmarks of Pegasus[97]. Moreover, while running Senator Brejza's European Parliament campaign, Senator Brejza's former assistant Magdalena Losko received four suspicious text messages in April 2019 which, according to Amnesty International forensic examiners, were technically consistent with the NSO Group's spyware Pegasus[98].

*ROMAN GIERTYCH*

69. Roman Giertych was targeted with Pegasus spyware during the last weeks of the 2019 parliamentary elections. Between September and December 2019, Giertych was hacked as many as 18 times, with most of the hacks taking place just before the date of the election, 13 October 2019. At that time, he was serving as the lawyer of leader of opposition party Civic Platform and former Prime Minister Donald Tusk. During that period, Giertych was also representing Radek Sikorski, the former Foreign Minister and current MEP with the European People's Party (EPP). Sikorski was bringing a case to investigate the involvement of Kaczynski and his allies in illegal wiretapping that resulted in the recording and publication of Sikorski's conversations[99].

70. As with the case of Senator Brejza, the government would neither confirm nor deny whether they were responsible for these attacks. It was reported by the Associated Press that a motion seeking the arrest of Giertych was filed by a prosecutor, regarding an alleged financial crimes investigation, just a matter of hours before state security spokesperson Stanislaw Zaryn responded to questions from the AP regarding the hacking of Giertych's phone. Giertych vehemently denies these allegations. Zaryn

---

[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.
[99] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 December 2021.

refused to comment on the possible connection between these incidents. In a similar incident, Giertych's home was raided and searched by CBA officials in 2020[100].

71. During this time in 2019, Giertych was also representing Gerald Birgfellner, an Austrian developer. Birgfellner had been involved in a construction project for PiS leader Jarosław Kaczynski, with whom he has family ties, when the deal was called off. Following the release of recorded conversations between the two, a political scandal erupted for Kaczynski who then cancelled the project. Birgfellner alleges that he was never paid for his services and so engaged Giertych[101]. Minister for Justice and Prosecutor-General Zbigniew Ziobro also commented in 2021 that he was seeking to bring charges against Giertych 'with the suspicion of committing crimes'[102].

*EWA WRZOSEK*

72. Prosecutor Ewa Wrzosek was the victim of hacking with Pegasus spyware as many as six times between 24 June and 19 August 2020[103]. Wrzosek is a member of Lex Super Omnia, an association of prosecutors working for the independence of the Prosecutor's Office. She was investigating the decision to hold the 2020 Polish presidential elections in the midst of the global COVID-19 pandemic when she was stripped of the case, which was subsequently dropped. It is within the powers of the Prosecutor-General, Zbigniew Ziobro, and his right-hand man, National Prosecutor Bogdan Święczkowski, to decide not to prosecute certain cases or to remove subordinate prosecutors from particular cases[104]. Afterwards, prosecutor Wrzosek was sent away, with only 48 hours' notice, to another prosecutor's office in a city several hours from her home. It was upon Wrzosek's return to Warsaw that she was targeted with Pegasus spyware. The Polish authorities have followed the pattern of declining to confirm or deny their responsibility[105] [106].

73. Wrzosek has also launched a legal complaint concerning the Pegasus infection of her mobile phone. The court ordered an expert opinion by Citizen Lab on the Pegasus infection and Wrzosek herself requested that her phone be checked by the experts of Citizen Lab. However, the prosecutor denied this request and selected another expert who was unable to link any infection to Pegasus. The prosecutor, moreover, requested the telecoms operator to hand over all metadata relating to Wrzosek for a period that is irrelevant to the court investigations. Wrzosek considers that she is still under surveillance and that the prosecutor's procedure is aimed at providing additional

---

[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.
[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 January 2022.

evidence that could be used against her in other cases[107].

74. As highlighted by Wrzosek during the PEGA Committee meeting of 19 January 2023, she is currently being charged by the Prosecutor's Office for revealing information on a case unrelated to Pegasus, and with being involved in political activity. Wrzosek is unable to build her legal defence, as the Prosecutor's Office is denying access to documents[108]. This appears to be a clear violation of the right to a fair trial, and creates the impression that the only purpose of the case is to discredit Wrzosek.

OTHER POSSIBLE TARGETS

*SUPREME AUDIT OFFICE*

75. Although not a target of Pegasus, the NIK – the Supreme Audit Office – which is tasked with safeguarding public spending and with the management of public services and which disclosed the invoices for the 'purchase of special technology means for detecting and preventing crime' for a total amount of PLN 25 million, was attacked and harassed by the Polish authorities. The timing of the attacks is particularly relevant given the nature of the investigation the NIK was conducting. The spokesperson for the NIK confirmed that it was investigating the cancellation of the presidential elections in 2020. The results of this probe saw the Prime Minister, members of his government and a Justice Ministry fund served with notifications of crimes. This appears to reinforce the suspicions that Pegasus has been used predominantly for political purposes in Poland[109].

*PIS ASSOCIATES*

76. It appears that Pegasus was used for the 'preventive wiretapping' of leaders and organisers of street protests against the reforms of the Constitutional Court implemented by PiS. However, it is not only opponents of the ruling party that may have fallen victim to Pegasus. According to sources cited by Wyborcza, former PiS party spokesperson Adam Hofman was spied upon in 2018, making him one of the first persons targeted following the purchase of the spyware. Hofman founded R4S, a PR company, after being expelled from PiS[110] [111]. Reportedly, this action agitated the ruling party and made Hofman a target for surveillance. He states that the information obtained about him was subsequently used in a smear campaign against him.

77. In addition, according to Wiadomości, former PiS Member of Parliament Mariusz Antoni Kaminski and former PiS Minister of the State Treasury Dawid Jackiewicz were allegedly targeted with Pegasus by the government[112]. Mariusz A. Kaminski was expelled from PiS after being embroiled in a scandal at the same time as Hofman, while

[107] PEGA Committee meeting, 19 January 2023.
[108] PEGA Committee meeting, 19 January 2023.
[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 October 2014.
[112] https://wiadomosci.onet.pl/kraj/pegasus-oto-kolejne-osoby-ktore-mialy-byc-inwigilowane-przez-sluzby-pis/yvt6tym.

Jackiewicz remains a member of the ruling party in spite of his sudden step back from his ministerial role[113].

78. A similar smear campaign was also conducted against the former President of the Employers of the Republic of Poland, Andrzej Malinowski, by the ruling party in February 2018. He testified before a special sitting of a Senate Committee in April 2022 regarding the hacking of his phone with Pegasus in order to collect the information for this public takedown[114]. He outlined that messages were taken from his WhatsApp and SMS using Pegasus and were strategically used to spread online hate against him. This attack was in retaliation for disagreeing with the ruling party and demanding alternative economic policies.

CONCLUDING REMARKS

79. The abuse of Pegasus in Poland has to be viewed in the full context of the rule of law crisis in the country, which began in 2015 when the government, led by PiS, started to dismantle the judicial system and has since systematically taken over the most important institutions in the country, installing party loyalists in all strategic offices. The ruling party purposefully and methodically put together the legal, institutional and political building blocks of this system to create a coherent and highly effective framework, where the use of Pegasus is an integral and vital component of a system for the surveillance of the opposition and critics of the government for political gain. It was designed to keep the ruling majority and the government in power.

80. The scope for surveillance in Poland has been expanded vastly over the past few years, weakening or removing safeguards and oversight provisions. In the course of systematic and targeted legislative changes brought about by the ruling majority, the rights of victims have been minimised and legal remedy and redress have been rendered meaningless in practice. Effective *ex ante* and *ex post* scrutiny, as well as independent oversight, have been *de facto* eliminated. Members of the Polish Government and party loyalists control the main positions within the system, directly or indirectly. The information harvested with spyware is used in smear campaigns against government critics and the opposition, through the government-controlled state media. The fact that the Polish Government has been broadening statutes in this systematic and targeted manner under domestic law keeps the legal basis for surveillance firmly in violation of EU law, the 2014 ruling of the Polish Constitutional Court and the fundamental rights of the Polish citizens. In this way, unlawful surveillance clearly violating EU and national law was essentially legalised.

*I.B. Hungary*

81. Hungary was one of the first countries to be embroiled in the European spyware scandal. In 2021, it was revealed by the Pegasus Project and confirmed by Amnesty

[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.

International[115] that over 300 Hungarians may have fallen victim to abuse with Pegasus, including political activists, investigative journalists, lawyers, entrepreneurs, an opposition politician and a former government minister.

82. In February 2023, a delegation of the PEGA Committee visited Hungary. It reached the conclusion that there is every indication that spyware has been grossly abused in Hungary and the authorities' explanation citing national security was deemed very unconvincing. Strong evidence indicates that people have been spied on with the objective of gaining even greater political and financial control over the public sphere and media market.

83. The committee was convinced that the rule of law and basic democratic standards have been seriously breached in Hungary and its situation is among the worst in the EU. As a result of years of democratic backsliding, state institutions do not seem to be geared towards serving citizens and protecting their rights and freedoms, but rather pursuing the political objectives of the government. The committee called on the authorities to allow a meaningful investigation of abusive practices.

PURCHASE OF PEGASUS

84. In 2017, the Hungarian Parliament's National Security Committee voted on allowing the country's intelligence services to acquire certain pieces of equipment by following the regular public procurement procedure. At the request of the Special Service for National Security (Nemzetbiztonsági Szakszolgálat, NBSZ), the Hungarian Parliament supported the acquisition of sophisticated spyware[116]. However, the procedure was secret and the requests for approval did not specify the specific brand and type of technology[117].

85. The Hungarian Ministry of the Interior bought Pegasus for EUR 6 million indirectly through Communication Technologies Ltd from NSO Group's company in Luxembourg in 2017, shortly after Prime Minister Viktor Orbán met with his Polish counterpart Mateusz Morawiecki and former Israeli Prime Minister Benjamin Netanyahu[118] [119]. The Hungarian Ministry of the Interior did not confirm this until November 2021 when the Chair of the Parliamentary Defence and Law Enforcement Committee, Lajos Kósa, acknowledged the purchase of Pegasus by the Fidesz government[120]. Kósa still insisted,

---

[115] Euractiv, 'Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 February 2022*.
[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] PEGA mission to Hungary, meeting with members of the National Security Committee of the Hungarian Parliament, 20-21 February 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 July 2021.
[120] DW, Hungary admits to using NSO Group's Pegasus spyware', 4 November 2021.

however, that the spyware had never been used against Hungarian citizens[121].

86. The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) inquired about the procurement procedure for the purchase of the spyware and received access to the secret contract with NSO. During the PEGA mission to Budapest in February 2023, the NAIH's President, Attila Péterfalvi, initially stated that it was not true that the provision of Pegasus to the Hungarian authorities had been terminated, which would mean that Hungary was not one of the two EU Member States that had been removed from the list of 14 to which NSO provides Pegasus. Péterfalvi later retracted his statement, maintaining that he had no information as to whether NSO had terminated the use of Pegasus in Hungary or not.

LEGAL FRAMEWORK

87. In Hungary, the framework for the legal interception of communications in the context of a criminal investigation is stipulated in the Police Act. According to the Police Act, the surveillance of private citizens in a criminal investigation can only be carried out with judicial approval. In matters related to terrorism, however, the Police Act refers to the investigatory surveillance mentioned in the National Security Act[122]. Under this provision, judicial approval does not have to be sought in order to approve the use of these techniques, but the Minister of Justice is responsible for providing the authorisation instead[123]. Requests for the authorisation of surveillance do not mention the type of technology that will be used[124].

88. Pursuant to Act CXXV of 1995, the national security interest is defined as 'ensuring the sovereignty, and protecting the lawful order, of Hungary, and within this framework', which is a rather broad definition.

89. In a landmark case (*Szabó and Vissy* v *Hungary*[125]), the European Court of Human Rights (ECtHR) found that the National Security Act did not provide for safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of surveillance measures. The National Security Act omits a requirement for the notification of surveillance subjects and it specifically stipulates that targets must not be informed by the authorising party that they are being spied on[126]. The requirement to notify victims was unequivocally established in the case of *Klass and others* v *Germany*[127] by the ECtHR. Moreover, there are no effective avenues for remedy and redress in the event of abuse and no proper oversight. The Hungarian Government has so far failed to implement either ruling.

---

[121] DW, Hungary admits to using NSO Group's Pegasus spyware', 4 November 2021.
[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] PEGA mission to Hungary, 20-21 February 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.

90. According to the National Security Act, surveillance carried out by the Special Services for National Security (SNSS) using spyware is dependent on the permission of the Minister of Justice in most instances, and on the judge designated by the President of the Metropolitan Court of Budapest in some specific cases[128] [129]. No appeal can be lodged against these decisions and there is virtually no oversight of the process[130] [131].

91. Despite the gravity of such a decision, when she is not available, the current Minister of Justice, Judit Varga, delegates responsibility for the authorisation of spyware use against citizens to the Secretary of State of the Ministry of Justice, a position currently held by Robert Repassy[132]. This was confirmed by Repassy himself in a response he authored to a written questions on the issue[133]. It is widely reported that Varga regularly passed on the responsibility to Repassy's predecessor Pál Völner, who was forced to resign from the role in December 2021 as a result of a major corruption scandal[134]. It was widely reported that he accepted millions of Hungarian forints in bribes from a number of high-profile stakeholders in return for favourable decisions and appointments to key positions by Völner in his capacity as Secretary of State[135].

92. While Interior Minister Sándor Pintér insists that this authorisation procedure through the minister or the courts is always followed without exception[136], the weak legal provisions of the National Security Act also make it possible for the directors-general of the SNSS to grant interim authorisation for surveillance to be conducted without consent until such time as official permission can be granted. This allows the SNSS to operate without any proper judicial authorisation as long as they claim that the delay in obtaining permission would harm their operation. In such cases, the unauthorised surveillance can continue[137].

93. The legal limit of a maximum of 90 days for surveillance imposed by the Act can be

---

[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 , July 2022 at pg. 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.

extended for a further 90 days upon a simple request from a director-general to the permitting officer[138], which is only provided for to give the appearance of a legal safeguard.

94. In addition, the role of the NAIH is to oversee all surveillance by the secret services. The NAIH's President, Attila Péterfalvi, has continuously asserted that all use of Pegasus was for national security purposes, which falls within the exclusive competence of national governments[139]. However, the NAIH only verified the authorisation procedure on technical grounds, in order to ascertain whether the processing of data was lawful, but did not look into the substance of the use of Pegasus. The NAIH did not see the necessity to call on the targets to testify, as the NAIH had access to all relevant documents. Only the cases authorised by the Minister of Justice were investigated, as the NAIH cannot investigate authorisations granted by a judge[140].
According to Péterfalvi, the NAIH investigation did not uncover any illegal activity or anything inconsistent with the terms of sale of the NSO Group[141].

95. The head of the NAIH is appointed by the Prime Minister, hence their independence can be called into question[142]. The ECtHR ruled on the matter in September 2022 in a case of *Hüttl* v *Hungary*[143] taken by Hungarian Civil Liberties Union (HCLU) lawyer Tivadar Hüttl when, after he had allegedly been wiretapped, the National Security Committee decided not to launch any further investigation and no more remedies were available[144]. The ECtHR stated in its judgment that the NAIH, though entitled to investigate the actions of the secret services, was incapable of conducting independent oversight of the use of surveillance. The court held that the NAIH lacked the necessary competence to do so, given that the secret services are entitled to deny access to certain documents on the basis of secrecy[145]. In such an instance, it would fall to the minister responsible for the secret services to conduct an audit, which could not be deemed independent oversight in any way[146].

*EX POST* SCRUTINY

96. In November 2021, on the insistence of the opposition, the National Security Committee and Committee on Defence and Security in the National Assembly conducted hearings into the use of spyware in Hungary and the alleged politically motivated targeting of citizens by the government in particular. The government party held 4 out of 6 seats in the National Security Committee and prevented any meaningful

[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] PEGA mission to Hungary, 20 February 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.

and democratic scrutiny of the use of Pegasus**.** The representatives of the government party insisted that all surveillance had been authorised through the appropriate channels, but refused to comment as to whether or not journalists or politicians had been targeted. They also refused to comment on the fact that the authorisations had been delegated by the Minister of Justice to the Secretary of State, Pál Völner, who is under investigation on charges of corruption and abuse of power. They also rejected requests from the opposition members to conduct an in-depth investigation and to visit the security services in order to conduct interviews with individual agents. Key targets, such as Zoltán Varga and Szabolcs Panyi, were not heard by the committee. In August 2021, only a pro forma, general investigation was conducted, as this was the only formula that obtained support from the majority[147]. It is not possible to know exactly what was said however, as the ruling party have classified the minutes of the meeting until 2050[148].

97. An NAIH investigation was launched following allegations by at least 10 lawyers, the President of the Hungarian Bar Association and at least five journalists who were being targeted[149]. The resulting report was published on 31 January 2022 and concluded that the use of Pegasus was strictly for reasons of national security.

98. Similarly, the Hungarian prosecution service closed its investigation into the targeting on 15 June 2022, concluding that no unauthorised surveillance had taken place.

99. Given that the power of authorisation rests with the Justice Ministry and the Fidesz-backed Prosecutor-General, Péter Polt, was re-elected in 2019 for a further nine years (having already served for a combined period of 15 years over two different terms up to that point), genuine oversight of the government can be called into question.

100. There is no support within the Hungarian anti-corruption framework in response to this, given that the Ministry of the Interior, which initially purchased Pegasus from the NSO Group, is responsible for the coordination of all anti-corruption policy and oversight[150].

REDRESS

101. When the Pegasus scandal erupted in Hungary, journalists were one of the groups most targeted by the government. As a result, in early 2022 a group of six journalists and activists initiated legal actions before the Hungarian authorities, the Commission and the EctHR. The Hungarian Civil Liberties Union (HCLU) is representing journalists Brigitta Csikász, Dávid Dercsényi, Dániel Németh and Szabolcs Panyi in addition to Adrien Beauduin, a Belgian-Canadian PhD student and activist. The sixth party has chosen to remain anonymous. The HCLU is also working with Eitay Mack in Israel to file a case with the Attorney General in order to trigger an investigation into the NSO

[147] PEGA mission to Hungary, meeting with members of the National Security Committee of the Hungarian Parliament, 20 February 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.

Group[151].

102. Many technicalities are blocking the path for this case in the Hungarian courts. Given that there is not a wealth of case-law in this area, the procedures are unclear. For example, issues regarding jurisdiction have arisen. Such actions and relentless delays are mainly viewed as attempts to have the case dismissed on a technicality or procedural issue.

103. There is also a serious issue regarding access to information. In order to request access to the files containing all of the data gathered on any individual citizen, it is necessary to provide the exact name of the file to which the request relates, information which it is almost impossible to acquire. With the requests of the six parties represented by the HCLU inevitably having been rejected by the Supreme Court, the HCLU sought a ruling from the Constitutional Court declaring this practice, and the ruling of the Hungarian Supreme Court, unconstitutional. However, in 2021, the Constitutional Court rejected the HCLU's motion.

104. In addition to its lawsuits before the courts, the HCLU has also pursued other avenues to access the data of its six clients. An administrative procedure was initiated and accepted under the Classified Data Act and the Data Protection Act. However, a year-long review will be carried out by the Constitution Protection Office in each individual case before any results will emerge[152]. Furthermore, the spyware attacks have been reported to the Commissioner for Fundamental Rights (Ombudsman). The Constitutional Court has stipulated that the responsibility lies with the Ombudsman to investigate abuses by the secret services[153].

105. In another attempt to achieve some transparency, the HCLU has requested access to the data being collected and processed as a result of the hacking of the six target persons in a process that is being conducted outside the court system. However, the entitlement to this information only exists so long as providing the data to the subjects does not interfere with national security[154]. This creates another pretext for the Hungarian authorities to once again fall back on national security reasons[155]. So far, the Constitution Protection Office has rejected 270 freedom of information requests submitted by the HCLU between 2018 and May 2022[156].

POLITICAL CONTROL

106. Political control over the use of surveillance in Hungary is complete. The Orbán-led Fidesz regime has created a system in which they can target lawyers, journalists, political opponents and civil society organisations.

107. The Minister of the Interior was responsible for the purchase of Pegasus spyware in the first instance, and the Minister for Justice remains in charge of authorising its use.

---

[151] The Guardian, https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state , *28 January 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.
[155] https://hclu.hu/en/pegasus-whats-new.
[156] https://hclu.hu/en/pegasus-whats-new.

Hungary's legislative framework regarding the surveillance of its citizens has repeatedly been found wanting. However, the ruling party will make no moves to alter it as it suits their own agenda.

108. The Prime Minister selects the head of the NAIH, the body responsible for the independent oversight of Pegasus use by the secret services. Given that he is a political appointee, independent oversight is absent. Hungary and the Fidesz government are no strangers to these types of political appointments. The government has systematically placed party loyalists in leading roles in bodies such as the Constitutional Court, the Supreme Court, the Court of Auditors, the prosecution service, the National Bank of Hungary and the National Election Committee[157]. This ensures that any institution created with the intent of conducting oversight of the executive branch cannot carry out its role in an independent manner[158].

109. With respect to the practical element of conducting surveillance through the use of spyware, telecommunications companies have a significant role to play. There are multiple instances of targets' devices being infected through links sent via SMS, and the wealth of data that telecommunications companies have access to is very attractive for those wishing to conduct surveillance. In the case of Hungary, the situation has become more dangerous, as the Hungarian Government recently bought telecom provider Vodafone Hungary[159]. With support from the Hungarian Government, the company 4iG bought 51 % of Vodafone through a subsidiary. In addition, the Hungarian Government bought 49 % of Vodafone's shares through another company. The links between 4iG and the government are evident. The current chair of the company was a close associate of Hungarian oligarch Lőrinc Mészáros, a childhood friend of Viktor Orbán. The total acquisition costs EUR 1.7 billion and will grant the government easy and direct access to the data of more than 3 million customers[160]. Moreover, owing to this purchase, the state will have an access point to the decades-old global messaging system known as SS7[161]. This system allows mobile operators to connect users around the world. The Hungarian state will also be able to lease out such an access point further, as was the case for Rayzone[162].

THE TARGETS

110. It was reported that the phone numbers of over 300 persons were included in the

---

[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.
[160] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22 August 2022; Volkskrant, Orbán verstevigt met overname 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.

findings of the Pegasus Project [163]. Among them were at least five journalists, 10 lawyers, the mayor of Gödöllő, who is a member of an opposition party, an employee of the opposition party, as well as activists and high-profile business owners[164]. However, none of them were the target of any criminal investigations or accused of anything. While the appearance of phone numbers on this list does not necessarily mean that the phones were actually hacked, it is a revealing insight into the methodical and systematic actions and attitude of Orbán's government towards fundamental rights and media freedom. Since that time in 2021, a number of targets have been confirmed as having been successfully hacked with spyware. From the moment that the spyware scandal broke in Hungary, it has been very clear that the government's actions were politically motivated.

*SZABOLCS PANYI*

111. The hacking of journalist and editor Szabolcs Panyi's phone occurred during the course of his work at Direkt36. As one of the few remaining independent news sources in Hungary, it is a major target of the ruling party. Panyi is a well-known, well-regarded journalist, so it follows that in addition to collecting key information directly from Panyi himself, many of the contacts and sources on his phone would be valuable by-catch for the government.

112. Amnesty International confirmed that Panyi's phone had been consistently hacked in 2019 over a period of seven months[165]. These attacks were pointed and often occurred at times when Panyi had requested the government to provide a comment on issues. A specific and troubling example of this occurred on 3 April 2019. Panyi contacted the government requesting a comment on the article he had written detailing the move of a Russian bank to the Hungarian capital, which was a high-profile story, given that there were questions about whether or not the bank was in fact a front for the Russian intelligence services[166]. Amnesty International confirmed that Panyi's phone was hacked the following day, and additionally verified that there were 11 other such instances of hacking in the immediate aftermath of a request for comment from Orbán's administration[167]. That equates to over half of Panyi's requests resulting in being targeted within that seven-month period[168].

113. The authorities have feigned ignorance about the targeting of Panyi and will neither confirm nor deny that they were responsible. However, the government has previously attacked Panyi publicly, with Orbán's spokesperson alleging that he was a fanatical

[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 July 2021 and 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.
[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.

political activist, as well as accusing him of Orbánophobia and Hungarophobia[169]. This is a blatant attempt to discredit Panyi and portray both his sources and himself as the 'enemy' through the government's own state-controlled media.

114. Following an investigation by Panyi into the Hungarian broker company Communication Technologies Ltd, through which Pegasus was purchased, the company sued him[170].

*ZOLTÁN VARGA*

115. As CEO and Chair of Central Media Group, Zoltán Varga is the owner of Hungary's largest remaining independent news site 24.hu. After the Orbán government initiated a takeover of its main competitor, Index.hu, in 2020, Varga was left as 'the last man standing' in defiance of the ruling party[171].

116. Fidesz has been conducting a smear campaign against Varga via the government-controlled media for some time in order to discredit both his personal public figure and the publication, in spite of its popularity, with an audience of over 7.5 million per month[172]. Varga alleges that he was both enticed and threatened to sell on different occasions, including offers for generous state advertising subsidies in return for hiring the government's choice of editorial staff[173]. Varga first suspected his phone was infected with Pegasus when he began hearing a playback of the call while in mid-conversation. Subsequently in 2021, it was discovered by Amnesty International that Varga had indeed most likely been hacked by Pegasus, but it could not be confirmed owing to the fact that the phone had since been replaced[174].

117. Additionally, shortly after the 2018 elections, the re-elected Orbán attempted to get to Varga indirectly. Following a dinner party to discuss the government's media takeover, hosted by Varga in spring 2018, which included Attila Chikán, a former Fidesz minister turned Orbán critic, it was verified that all those present were recorded as being candidates for surveillance[175]. It was subsequently confirmed that one guest was hacked at the time of the party, while other phones showed traces of potential Pegasus hacks but no proof of successful infection[176]. The hacking was all but confirmed by a government-affiliated acquaintance of Varga's, who directly referenced the dinner party in conversation and warned against socialising with people who could be

[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] PEGA mission to Budapest, 20-21 February 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.
[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.

'dangerous'[177].

118. Varga has also been the subject of traditional surveillance. Eavesdropping in the business setting, cars lingering outside his home and helicopters hovering over his home, and several incursions into his garden, have warranted him engaging full-time security.

119. In October 2022, criminal charges were launched against Varga. He was called in for questioning by the police and just minutes later the government-friendly media were already reporting about it[178].

*ADRIEN BEAUDUIN*

120. Adrien Beauduin appeared on the radar of the Orbán regime in 2018 while completing a PhD in gender studies at the Central European University. The institution was founded by George Soros and the government was trying to remove it from Hungary at the time, along with the entire subject of gender studies[179]. After attending a protest in Budapest, Beauduin was arrested in what is seen as a highly politically motivated move, and faced charges for assault of a police officer, which he vehemently denies[180]. It was reported that there was essentially no evidence against Beauduin, and the evidence that was submitted had been copied verbatim from the police testimony in another case[181]. In 2020, the criminal proceedings against Adrien Beauduin, who was represented by the HCLU in the case, were terminated.

121. Government representatives publically condemned the so-called pro-immigration Soros network for orchestrating 'violent demonstrations in Budapest'[182]. Subsequently, traces of Pegasus were found on Beauduin's phone, but it was not possible to confirm whether there had been a successful infection.

122. Given that Beauduin was a Belgian citizen living in Hungary at the time of these incidents, the importance of the cross-border dimension of this case cannot be overstated. It is critical, as it affects the sovereign rights of EU citizens, such as freedom of movement and the right to work. The Commission has a complaints procedure in place that any person can avail of if their Charter rights have been breached. Adrien Beauduin lodged such a complaint on 24 January 2022. However, seven months later, in a letter of response dated 17 August 2022 addressed to his lawyer, the Commission claimed it does not have the competence to intervene[183].

---

[177] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 July 2021.
[178] PEGA mission to Budapest, 20-21 February 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.
[180] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[181] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[182] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[183] https://tasz.hu/a/files/220816-Complaint-unlawful-surveillance.pdf.

*ILONA PATÓCS*

123. Lawyer Ilona Patócs was a suspected victim of Pegasus surveillance in the summer of 2019 while she was representing a client in a high-profile, long-running murder case[184]. However, owing to the type of mobile device she was using, it was not possible to confirm whether the hack was fully successful or exactly when it occurred. Her client, István Hatvani, had already served seven years for an assassination, which Patócs claims was a 'politically motivated' conviction[185]. Despite another party later claiming responsibility for the murder, the Hungarian Court of Appeal sent Hatvani back to prison to complete his original sentence. Many other lawyers' phone numbers have been listed as potential targets of Pegasus, including President of the Hungarian Bar Association János Bánáti[186]. This targeting in particular shows a clear disregard by the government for the privilege that exists between lawyers and their clients.

*GYÖRGY GÉMESI*

124. György Gémesi, the mayor of Gödöllő, was also targeted by the Pegasus spyware at the end of 2018, just as he was under severe pressure from the government and unknown persons broke into both his and his children's homes. At the same time as the opposition mayor, at the end of 2018, a government acquaintance of Gémesi was also selected as a target of the spyware. In addition, two phone numbers linked to his party colleagues and Gémesi's former deputy mayor also appeared on the list.

*BRIGITTA CSIKÁSZ*

125. During her surveillance, Brigitta Csikász, one of Hungary's most experienced crime reporters, was investigating the misuse of European Union funds among other topics. Csikász's investigations revealed that, in spite of the European Anti-Fraud Office (OLAF) sounding the alarm bells, the Hungarian authorities lacked either the will or the ability to prosecute the suspicious spending of EU money, proving yet again that while the prosecution is de jure independent and highly hierarchical, the chief prosecutor de facto closely linked to the government party and the Prime Minister.

126. President of the Hungarian Bar Association, János Bánáti, criminal defence lawyer and several other lawyers were also targeted with Pegasus.

OTHER TARGETS

127. People inside the ruling party's circle have also been targeted with spyware. The independent Hungarian outlet Direkt36 reported in December 2021 that the head of the protection service and the personal bodyguard to János Áder, the President and close ally of Orbán, had been hacked with Pegasus spyware. Direkt36 journalist and victim of

[184] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/ , 31 March 2022.
[185] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/ , 31 March 2022.
[186] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/ , 31 March 2022.

spyware Szabolcs Panyi has reported that this kind of spying is mainly as a result of the growing paranoia of the Hungarian Prime Minister. Cecília Szilas, former ambassador of Hungary to China, was targeted with Pegasus shortly before becoming senior advisor to Viktor Orbán. Attila Aszódi, state secretary of the Orbán government, responsible for the construction and development of the Paks II Nuclear Power Plant to be built by Roszatom, was also targeted by the Pegasus spyware. He became a target in 2018, while he was part of the government, but he had conflicts with his superior, Minister János Süli.

128. Furthermore, both the son and lawyer of one of Orbán's oldest friends, Lajos Simicska, were hacked with Pegasus[187]. Simicska went from being a close friend of Orbán to being an opponent. He was in the process of selling his media consortium that had fuelled much of the feud following Orbán's electoral victory in 2018 when this relational targeting occurred[188]. Simicska himself was not a target for the simple reason that he does not use a smartphone, thus rendering infection through spyware such as Pegasus impossible[189]. Ajtony Csaba Nagy, Simicska's lawyer, suspected an infection when he heard a playback of his conversation with Simicska during a phone call. Later, those suspicions were seemingly confirmed when information only discussed on those calls appeared in the Hungarian media[190]. Given that the majority of news outlets in Hungary are state owned, it is likely that the government itself provided the information directly to the media.

SPYWARE COMPANIES

129. The Hungarian Government has not only purchased and utilised Pegasus spyware against its people, but has also been playing host to other companies in the intelligence market such as Black Cube and Cytrox. Black Cube is an Israeli private intelligence agency comprised of former employees of Mossad, the Israeli military and Israeli intelligence services[191]. Their own company website dubs them as a 'creative intelligence service' finding 'tailored solutions to complex business and litigation challenges'[192]. Black Cube have been involved in a number of public hacking controversies including in the US and Romania[193]. Criticallylinks have also been uncovered with the NSO Group and Pegasus spyware. After much public pressure regarding NSO hiring Black Cube to target their opponents, former NSO CEO Shalev Hulio admitted to hiring Black Cube at in at least one situation in Cyprus.

---

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

130. Black Cube became involved in Hungary during the 2018 elections, when they spied on various NGOs and persons who had any connection to George Soros and reported back to Orbán in order for him to spin their activities in a smear campaign[194]. Those targeted included lawyer and member of the leading human rights NGO Hungarian Helsinki Committee, Marta Pardavi[195]. The resulting information from the surveillance of these individuals and NGOs appeared not only in the Hungarian state-controlled media, but also in the Jerusalem Post[196].

131. An additional connection with Hungary is Cytrox Holdings Zrt., which is registered to an address in Budapest. Cytrox, the creator of Predator spyware, was originally founded in North Macedonia, before it was bought by WiSpear, which is now part of the Intellexa alliance run by Tal Dilian.

CONCLUDING REMARKS

132. The use of Pegasus in Hungary appears to be part of a calculated and strategic campaign to destroy media freedom and freedom of expression by the government[197]. The government has utilised this spyware in order to usher in a regime of harassment, blackmail, threats and pressure against independent journalists, media, political opponents and civil society organisations with ease and without fear of recourse. The government's control over almost all offline and broadcast Hungarian media outlets allows it to continue pushing its own version of the truth, stopping much of the public scrutiny conducted by the independent media from reaching Hungarian citizens.

133. The law authorising the use of interception is much more of a tool of control and exercising power for the government than it is a shield for citizens' rights and privacy, and is one of the weakest in Europe[198] [199]. The system exists in blatant violation of the European requirements and standards pertaining to the surveillance of citizens in the European Convention on Human Rights and the rulings of the ECtHR[200] despite the government's insistence that it has acted legally in all instances and complies fully with the law[201] [202]. Although the government consistently falls back on reasons of 'national security'[203], its claims that the target persons are a threat to national security are not

[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.
[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] See, inter alia, 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 February 2022.
[203] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 February 2022.

credible.

*I.C. Greece*

134. The Committee visited Greece in November 2022 as part of a Greece-Cyprus joint mission. Members met Minister of State Giorgos Gerapetritis and discussed high-profile surveillance cases and the larger context of media pluralism and the rule of law in Greece. They also met investigative journalists, Members of the Hellenic Parliament, the President of the Hellenic Data Protection Authority (HDPA), representatives of the ADAE and NGOs, and human rights defenders.

135. The visit brought to light the fact that increased efforts must be made to ensure transparency. The allegations of abuse of surveillance and the use of spyware have to be thoroughly investigated and sanctioned where necessary. All necessary safeguards should be put in place and reforms should improve transparency and ensure appropriate judicial oversight of the use of surveillance. The visit also confirmed that clear rules were needed for limiting the use of national security as grounds for surveillance, ensuring proper judicial oversight and guaranteeing a healthy, pluralist media environment.

136. Throughout 2022, Greece was shaken by a series of reports regarding the use of spyware, which is illegal under Greek law. On 26 July 2022, Member of the European Parliament and leader of the Greek opposition PASOK party Nikos Androulakis filed a complaint with the Supreme Court Prosecutor's Office about attempts to infect his mobile telephone with Predator spyware[204]. The attempted infection with spyware was discovered during a check of Mr Androulakis's telephone by the European Parliament's IT service[205]. According to forensic analysis of the IT service, the hacking attempts happened while Mr Androulakis was a candidate for the leadership of the opposition party. This revelation brought into the spotlight complaints filed earlier in April and May 2022 by financial journalist Thanasis Koukakis regarding the infection of his telephone with Predator. His infection was confirmed by CitizenLab. In September, former Minister of Infrastructure and lawmaker for the Syriza party, Christos Spirtzis[206], also claimed to have been targeted with the Predator spyware. Although his mobile telephone was not officially checked, Mr Spirtzis did share the links he received with two technicians who verbally confirmed that he had been targeted[207]. Furthermore, it was revealed later that month that Greece's National Intelligence Service (EYP) had allegedly targeted two of its own employees with spyware[208]. On 5 and 6 November, the Greek media revealed a list of 33 targets of Predator, all of whom were high-profile personalities[209]. The list – neither confirmed nor denied by the government or by those surveilled – includes names of people working in politics, business and media in Greece. The impact of the alleged surveillance of people that appear on the list could be more extensive, as all their respective contacts and connections could also be 'caught'

[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.

indirectly in the spying operation, including their contacts in EU bodies. The high prevalence of spyware was reportedly already visible in the 2021 Meta report, which mentions 310 fake website links related to the Cytrox spyware company in its annex, 42 of which were set up to mislead targets in Greece alone[210] [211]. At the end of November 2022, Greek newspaper *Documento* published a list of 498 URLs that had been used to spy with Predator spyware. Some of the URLs were identical to those published by the 2021 Meta report[212]. On 28 February 2023, the President of the HDPA confirmed that 300 text messages related to Predator spyware had been sent to approximately 100 devices. The President of the ADAE additionally stated that the ADAE had acted upon several complaints and identified two instances of the use of Predator and one bank account number of a person behind the false text messages. The ADAE investigation into new complaints is ongoing[213].

137. In August 2022, the Greek Government conceded that the EYP had indeed been monitoring Mr Androulakis and Mr Koukakis, but it denied that it had ever used or purchased Predator spyware. In addition, other cases of surveillance by the EYP came to light during this period, such as that of journalist Stavros Malichoudis[214]. To date, the official reasons for the surveillance have not been disclosed.

138. On 8 August 2022, Prime Minister Mitsotakis issued a video message stating ambiguously that the surveillance of Mr Androulakis had been 'legal' but 'politically unacceptable'. He made no reference to the surveillance of Mr Koukakis, nor to the other alleged cases. He also stated that he had not been aware of the surveillance, but had he known, he would not have allowed it[215]. According to the official statement from the government spokesman Yiannis Oikonomou, as soon as the Prime Minister became aware of Mr Androulakis's 'legal interception', Minister of State Giorgos Gerapetritis sought to fully inform Mr Androulakis in private about the reasons behind his surveillance[216]. Mr Androulakis turned down the offer to be informed, stating that a private briefing such as that would be illegal and that the only lawful course was through the Greek Parliament. Later on, while testifying before the Parliament, Minister Gerapetritis declared that he had never been aware of the reasons and asked for any relevant information to be kept strictly secret. The EYP is under the direct control of Prime Minister Kyriakos Mitsotakis following a legislative amendment, which was adopted soon after his party Néa Dimokratía came to power in 2019[217].

139. After the revelations, Grigoris Dimitriadis, the government's General Secretary responsible for cooperation between the Greek Government and the EYP, and EYP

---

[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] PEGA Committee exchange of views with Konstantinos Menoudakos and Christos Rammos, 28 February 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 Predatorgate. 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.
[217] Euractiv, Another Greek opposition lawmaker victim of Predator.

director Panagiotis Kontoleon, resigned[218].

PURCHASE

140. At the end of 2019, Secretary-General Dimitriadis was in contact with NSO Group in order to purchase the Pegasus spyware. In January 2020, an official proposal submitted by NSO Group concerned a government-to-government agreement of EUR 50 million. After the signing of the agreement, the individual was to withdraw and the EYP was to take over. The EYP would cooperate with the Mossad for the installation of the system. The arrangement was eventually called off[219].

141. Both the EYP and the government categorically deny that Predator has ever been purchased or used by the Greek authorities[220].142. In the absence of any evidence on the identity of the buyer and user of Predator in the Greek cases, it cannot be established with certainty if or how the government or another actor had acquired Predator. If it was not the Greek Government, then it must be concluded that a non-state actor was responsible for the (attempted) hacks of the telephones of Mr Koukakis and Mr Androulakis. That would be a crime under Greek law, which would have to be investigated. The hypothesis that private actors were behind the Predator attacks is, moreover, highly implausible, as it would not explain the choice of targets. However, in principle it is not impossible to acquire or make use of spyware without government bodies actually directly purchasing the software. Spyware may be bought via proxies, broker companies or middlemen, as we have seen in other cases, or arrangements may be made with spyware vendors to provide certain spyware-related services. There is no doubt that there were close connections and interdependencies between certain persons and events relating to the government, the EYP and the providers of spyware, notably Krikel, a preferred supplier of communications and surveillance equipment to *i.a*. the police and the EYP. Krikel is closely connected with persons from the entourage of Prime Minister Mitsotakis. There is increasing evidence of the extensive relations between Intellexa, the company that owns Predator spyware, and the Greek State. On 16 January 2023, the Hellenic Data Protection Authority fined Intellexa EUR 50 000 for failing to cooperate and refusing to hand over information about its clientele, as part of its investigation launched in July 2020 following Mr Androulakis' complaint. The investigation is still ongoing[221].

143. One possibility is that Predator was acquired through Ketyak, the Centre for Technological Support, Development and Innovation set up by former Director-General of the EYP Kontoleon. It operates independently from the EYP[222] and participates in projects surrounding research, innovation and technology development[223].

THE TARGETS

[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 Predatorgate. The latest chapter in Europe's spyware scandal?.
[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.

*GRIGORIS DIMITRIADIS*

144. Dimitriadis is the nephew of Prime Minister Mitsotakis and until August 2022 he was Secretary-General in his office. In that role, he was responsible for government contacts with the EYP. He was forced to resign on 5 August 2022 following the revelation that the EYP had wiretapped the telephone of Mr Androulakis. Initially, his resignation was attributed to the toxic political environment but later on the Prime Minister attributed to him the political responsibility for the wiretapping of Mr Androulakis and other politicians[224].

145. The former head of the EYP, Panagiotis Kontoleon, admitted to the Greek Parliamentary Inquiry Committee his 'social relationship' with Mr Dimitriadis. Mr Kontoleon was appointed by the Mitsotakis government, but some provisions of the law had to be adapted so as to enable his appointment[225].

146. Mr Dimitriadis is also closely connected in several ways to Felix Bitzios and Giannis Lavranos. The three men are personally acquainted. Mr Dimitriadis and Mr Lavranos were each other's best men ('Koumbaroi')[226] and Mr Dimitriadis is the godfather of Mr Lavranos' second child[227]. Mr Dimitriadis was also indirectly connected to Mr Bitzios through business transactions with Mr Bitzios' brother[228].

147. This puts him at the heart of a network connecting him professionally as well as personally to key persons at Intellexa, Krikel and EYP.

148. Mr Dimitriadis is also reportedly acquainted with Andreas Loverdos, candidate for the PASOK-KINAL leadership in 2021.

*FELIX BITZIOS*

149. Business man Felix Bitzios had been implicated in the huge Bank of Piraeus violation of capital controls scandal. Pending the investigations, Mr Bitzios' assets had been frozen[229]. Mr Bitzios benefited from a legislative amendment introduced by Prime Minister Mitsotakis soon after he came to power in 2019. The controversial amendment set a time limit on the freezing of assets, thus enabling the release of frozen assets after a maximum of eighteen months[230]. Thanks to the amendment of the Mitsotakis government, the assets of Mr Bitzios could be released.

150. Mr Bitzios is connected with Cyprus through his company Santinomo, registered on Cyprus, and his connection with Tal Dilian. It seems that Mr Bitzios has been instrumental in the transfer of Intellexa to Greece[231].

---

[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.
[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.

151. Mr Bitzios owned 35 % of the shares of Intellexa through his company Santinomo. However, on 4 August 2022 he registered the transfer of all his shares to Thalestris, the mother company of Intellexa[232]. The date of the registration of the transfer took place a few days after the revelations of the Androulakis hack. However, the transfer itself supposedly took place on 28 December 2020, over 19 months earlier. Mr Bitzios thus retroactively distanced himself from his one-third Intellexa ownership. Nevertheless, Mr Bitzios had been connected to Intellexa from March 2020 to June 2021 as a deputy administrator[233].

*GIANNIS LAVRANOS*

152. Giannis Lavranos had been charged with tax evasion and journalist Mr Koukakis had been reporting on Mr Lavranos' case.

INTELLEXA

153. Predator spyware is sold via Intellexa, a consortium of spyware vendors with presence in *i.a.* Cyprus, Greece, Ireland and France. Tal Dilian, who had a former career in the Israeli Defence Force, set up the consortium in Cyprus. His second former wife and Polish citizen Sara Hamou is a central figure in the intricate network of companies. Tal Dilian also has acquired Maltese citizenship. The Greek Government declared that two export licenses had been granted to Intellexa , one of which authorised the export to Madagascar. In addition, the Greek Government issued an export license for Predator to Sudan. It has not been confirmed to whom the license was issued, whether to Intellexa or another entity.Intellexa has reportedly also exported its products to Bangladesh.

154. On 30 November 2022, an investigative report by Lighthouse Reports, in collaboration with the Israeli newspaper *Haaretz* and the Greek outlet Inside Story, revealed that Tal Dilian's Predator operations in Greece were allegedly connected to a Cessna jet flying from Greece and Cyprus to Sudan between April and August 2022. Reportedly, this jet secretly and illegally delivered high-end surveillance technology to the Rapid Support Forces (RSF) militias[234]. Flight records linked the private jet, flying in and out via Cyprus, to Tal Dilian, a former senior Israel Defence Force operative who set up Intellexa Alliance in 2019 with bases in Cyprus and Greece. On 18 February 2023, the Commission confirmed that it had contacted the national authorities in Greece and Cyprus for clarification of this matter. However, the Commission has not received an answer[235]. On 19 April 2023, the Greek Alternate Foreign Affairs Minister Miltiadis Varvitsiotis confirmed that the Greek Government had approved the license for the export of Predator spyware to Sudan. The minister, however, denies any role of Predator in the recent clashes between the Sudanese armed forces and the RSF militias

[232] Inside Story, Predatorgate: The second shareholder of Intellexa SA.
[233] https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae.
[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; PEGA Committee Meeting, 28 March 2023.

in Sudan[236].

155. In December 2022, the Greek Government disclosed that it had provided Intellexa with two export licenses on 15 Novembe 2021. According to the spokesperson for the Greek Foreign Ministry Alexandros Papaioannou, one of these licenses authorised the sale of Predator to Madagascar[237]. The licence was granted despite the country's poor human rights record[238] and potentially being in conflict with the EU Dual Use Regulation[239]. Secretary-General of International Economic Relations Ioannis Smyrlis – who authorised the sale of Predator to Madagascar – handed in his resignation after these revelations came to light[240] to take up the post of deputy director-general of the ruling party Néa Dimokratía, which is responsible for the upcoming elections.

156. In addition to the export of spyware, one case reportedly shows that Greece hosted training trips for the use of spyware. In June 2021, Bangladesh purchased a spyware vehicle from the Cypriot Passitora firm. According to documents from the Ministry of Home Affairs of Bangladesh, the personnel of the National Telecommunication Monitoring Centre (NTMS) were trained in Greece between 2021 and 2022 to use the spy vehicle. The vehicle eventually arrived in Bangladesh in June 2022[241].

KRIKEL

157. Krikel is a preferred supplier of equipment to the Greek law enforcement and security authorities. It is also the Greek representative of RCS Lab, an Italian company selling surveillance software. In addition, Giannis Lavranos is said to be a 50 % owner of Krikel, through another company called Mexal[242]. However, it does not seem to be possible to establish with certainty who is the ultimate beneficial owner of Krikel, despite its many contracts with state authorities.

158. In 2014, Giannis Lavranos' company Ioniki Technologiki was sold to Tetra Communications in London. In this same year, Ioniki Technologiki was one of the three companies that donated the Tetra Communications Systems to the Greek Ministry of

---

[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'.
[241] *Haaretz*, 'Israeli Spy Tech Sold to Bangladesh, World's Third-largest Muslim Country, Despite Dismal Human Rights Record'.
[242] There are several connections of interest here. Lavranos sold his in Athens-based family home at a price below market value to Albitrum Properties in April 2021. The representative of Albitrum Properties during the sale was Felix Bitzios' half-brother Theodoros Zervos. Albitrum is a Cypriot company and has as its shareholder Mexal Services Ltd. Mexal Services owns 100 % of Eneross Holdings Ltd. Eneross Holdings in addition owns Krikel. Giannis Lavranos' registered office is at the same address as Eneross Holdings and Mexal Services in Cyprus. See: Inside Story, 'Predatorgate's invisible privates', and TVXS, 'G. Lavranos behind KRIKEL – How the deception of the Parliament was attempted [Revealing documents]'.

Citizen Protection[243]. In 2014, the Greek Government had also shown interest in the Italian spyware brand called RCS Galileo from the company Hacking Team, as revealed by Wikileaks, but this software was never acquired[244]. The donation of Tetra was facilitated by a Florida-based company, allowing the regular tender procedures to be bypassed. The donation to the Greek Government was accepted in 2017. In 2018, Krikel signed a maintenance and technical support contract of EUR 10.8 million. Krikel administrator Stanislaw Pelczar signed on behalf of Krikel, but it seems that Lavranos was informally involved in the negotiations throughout[245]. Krikel became an important supplier of the Greek Ministry of Citizen Protection. Since 2018, it has signed seven contracts with the Greek Government, six of which are secret[246].

159. The Krikel company also became the local representative of the Italian company RCS Lab. In June 2021, the EYP reportedly purchased a wiretapping system from RCS lab[247] through Krikel[248]. At that time, Dimitriadis was responsible for the contacts between the government and the EYP. Some sources have documented that it was during the installation of this new system that material containing information on the surveillance of Androulakis and Koukakis was lost, allegedly caused by a technical problem[249]. Other sources, however, claimed that Kontoleon had ordered the destruction of files on 29 July 2022[250].

160. Interestingly, employees of Krikel have been spotted working at Ketyak, allegedly 'pro bono'. Ketyak has reportedly been granted EUR 40 million from the EU's Recovery and Resilience Facility, through a confidential tender procedure based on a secret decision of the Prime Minister[251]. Unlawful use of EU funds to finance illegal spyware would constitute a severe violation of Union law and would fall within the competences of numerous European bodies, including the European Prosecutor's Office.

161. Reportedly, Krikel employees also visited EYP facilities in Agia Paraskevi in December 2021 and January 2022 in their role as 'trainer'. These facilities are controlled by the Greek Government and are allegedly the place where the Predator spyware was installed[252].

INVOLVEMENT OF BITZIOS AND LAVRANOS

162. Bitzios and Lavranos were both actively involved in the setting up of Krikel in 2017. Together they arranged the appointment of Polish lawyer Stanislaw Pelczar as the

[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] *Hellas Posts English*, 'The EYP supplier contaminates smartphones in Greece as well'.
[248] TVXS, 'G. Lavranos behind KRIKEL – How the deception of Parliament was attempted [Revealing documents]'.
[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'.

administrator of Krikel in October 2017[253]. Bitzios' company Viniato Holdings Limited was subsequently hired as a consultant by Krikel between January and August 2018 for a fee of approximately EUR 550 000 (although Krikel only had a turnover of EUR 840 000 that year)[254].

163. Bitzios and Pelczar have other mutual business connections as well. It emerges from the Paradise Papers that they share a company registered in Malta by the name of Baywest Business[255]. In addition, Tal Dilian, the founder of Intellexa, holds a Maltese (golden) passport[256] and also has a letterbox company MNT Investments LTD in the island state[257].

164. Bitzios and Lavranos are two key figures in the supply of communication and surveillance material to state bodies such as the police and the EYP. Bitzios was pivotal in the company that sells Predator. They were close to Dimitriadis and they both benefited from lucrative government contracts. They benefited from the new government's legislative amendment releasing their frozen assets. They had a motive for using spyware against Koukakis. There is a very obvious and high risk of conflicts of interest and corruption in the entanglement of business interests, personal relations and political connections. They would, moreover, be in a position to provide crucial information about the acquisition and use of Predator in Greece.

165. Yet, despite the obvious relevance of Bitzios and Lavranos testifying before the Inquiry Committee of the Greek Parliament, the Néa Dimokratía majority on the committee rejected the requests of the opposition to summon these individuals for a hearing.

*EX ANTE* SCRUTINY

166. In Greece, infecting a device with spyware is a criminal offence, as stipulated in several articles of the Greek Criminal Code, including Article 292 on crimes against the security of telephone communications, Article 292B on hindering the operation of information systems, as well as Article 370 on violations of secrecy of letters. In addition, the production, sale, supply, use, importation, possession and distribution of malware (which includes spyware) is also a criminal offence, as outlined in Article 292C of the Greek Criminal Code[258]. This article was changed by the Greek Government on 9 December 2022.

167. The number of authorised wiretaps has increased substantially over the years. From 4 871 in 2015, to 11 680 in 2019 to 15 475 in 2021[259]. Currently, some 60 requests have

[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.
[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"'.

to be processed each day, until recently by a single prosecutor. Moreover, the provisions of the EYP that lift the confidentiality of citizens' communications for reasons of national security do not mention the name of the person concerned or the reason for the lifting of confidentiality. They are limited to the telephone number and the invocation of national security[260].

168. The judicial authorisation to monitor private communications, as well as the extension and the termination of such an authorisation, have to be approved by the competent Public Prosecutor. As stipulated in Law 3649/2008, the competent prosecutor to lift secrecy and confidentiality is the in-house prosecutor of the EYP. A legislative amendment from 2018 under the Tsipras II government had reduced the number of prosecutors required for the authorisation of a wiretap from two to one. The prosecutor in charge of the cases at hand is Vasiliki Vlachou[261]. Vlachou did not meet with the PEGA mission to Greece.

ACT OF LEGISLATIVE CONTENT

169. Following the surveillance revelations, Prime Minister Mitsotakis has proposed changes to the EYP's framework of operation. One of those changes is the introduction of the Act of Legislative Content by the government on 9 August 2022. Paragraph 2 of Article 9 of Law 3649/2008 is updated and now requires an opinion of the Permanent Committee on Institution and Transparency on the appointment of the EYP governor[262]. However, as the governing party currently has an absolute majority in the Parliament's Special Permanent Committee on Institutions and Transparency, it endorsed the nomination of Mr Demiris as the new EYP governor, while all other opposition parties were against[263]. Incidentally, the second deputy commander of the EYP is Dionysis Melitsiotis[264], a former member of the private office of the Prime Minister, and another Deputy Director is Anastasios Mitsialis, a former Néa Dimokratía official[265].

170. In addition, the act reintroduced the two-prosecutor authorisation of monitoring requests[266]. Article 5 of Law 3649/2008 on the provision for the lifting of confidentiality of communications by the EYP is supplemented with a submission for approval to the competent Prosecutor of Appeals, and after that, approved by the Public Prosecutor of the Court of Appeals[267].

*EX POST* SCRUTINY

171. Since 2019, the actions of the EYP have been under the direct control of Prime Minister

[260] Reporters United, 'Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis'.
[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?'.

Kyriakos Mitsotakis, after a change in the law following the victory of Néa Dimokratía in 2019[268].

172. Parliamentary control is exercised by the Permanent Committee on Institutions and Transparency. This committee supervises the actions of the EYP and has the power to collect documents, examine persons and invite the Director-General for a hearing[269]. The governing party has an absolute majority in the current committee composition.

173. The Hellenic Authority for Communication Security and Privacy (ADAE) ensures the protection of confidentiality of mail and all other sorts of communications[270]. The statute of ADAE grants it administrative autonomy[271]. ADAE can carry out investigations at facilities, databases and archives, and of the technical equipment and documents of the EYP[272].

174. The confidentiality of communications as provided in Law 2225/1994 states that this confidentiality may be waived solely in cases of national security and for inquiries into serious crimes. After the lifting of confidentiality, Article 5 of this law stipulates that the ADAE can inform the targets of the investigations, provided that the purpose of the investigation is not compromised[273]. The right of an individual to have access to information on whether the person in question has been the object of surveillance is outlined in Law 2472/1997[274]. However, when in March 2021 the ADAE notified the EYP about the right of Koukakis to be informed, the government immediately submitted Amendment 826/145 on 31 March 2021, which abolished the ability of the ADAE to notify citizens of the lifting of the confidentiality of communications[275]. This de facto strips the individual of their right to information. The amendment was introduced in a highly irregular manner. It was added to an unrelated law (a bill to do with COVID-19 measures) and the deadlines required by the Constitution were not respected[276] [277] [278]. There was therefore no proper consultation process.

175. With the Act of Legislative Content, Mitsotakis aimed to strengthen transparency and accountability. However, the act does not revoke Amendment 826/145.

176. On 9 December 2022, the Greek Government adopted Law 5002/2022 with the aim of updating and creating an effective legal framework for the protection of personal data, communication secrecy and the strengthening of cybersecurity. However, the law introduces several provisions that weaken safeguards, scrutiny and accountability. As

---

[268] Euractiv, 'Another Greek opposition lawmaker victim of Predator'.
[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'.

stipulated in Article 4, Paragraph 7[279], any request by individuals for information on whether they have been subject to surveillance for national security reasons will be examined by a three-member committee composed of the director of the EYP, the prosecutor attached to the EYP and the head of the ADAE. This means that the majority rests with those who ordered (director of the EYP) and authorised (prosecutor) the surveillance in the first place. Additionally, it makes it practically impossible for individuals who are under surveillance on national security grounds to be appropriately informed *ex post*, as the law stipulates that they may file a relevant request only three years after the termination of their surveillance. This is incompatible with the relevant jurisprudence of the European Court and the European Charter of Human Rights[280] and it does not provide for institutional checks and balances to ensure the proper functioning of state powers. The ADAE has expressed its disagreement with the three-member body. To date, there is no operational framework for the tripartite committee, which means it is de facto not functioning[281]. In addition, the new law criminalises the use of spyware by individuals or private companies, and for the first time makes it legal for public authorities to purchase spyware, authorising the government to set up the procedure via a Presidential Decree. There is no provision for judicial oversight of spyware use, or for subcontracting wiretapping to private entities.

177. The supply by private actors of spyware is only illegal if such software is included in an indicative list of 'prohibited spyware' that is updated by the Head of the EYP every six months. It authorises the EYP to acquire spyware legally, since critical relevant issues will be exclusively dealt with via secondary legislation (i.e. a Presidential Decree). Therefore, an updated version of existing spyware will be considered legal until included in the abovementioned list. The definition of 'national security' in the law is extremely broad and vague, thus in conflict with Article 19, paragraph 1 of the Constitution, which calls for a narrow interpretation. The ADAE is further obstructed in its efforts to exercise its constitutionally designated role in controlling the declassification process. The role of the independent authority that was instrumental in uncovering the surveillance scandal is downplayed in the new law, despite the relevant constitutional guarantees.

178. The possibilities for *ex post* scrutiny were weakened by the fact that Greece took a long time to fully implement the EU Whistleblowers Directive[282]. On 27 January 2022, the Commission launched an infringement procedure by sending a formal notice to Greece.

---

[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] PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos, 28 February 2023.

[282] https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768.

On 15 July 2022[283], the Commission sent a reasoned opinion with a deadline of two months to reply. The Greek Parliament eventually voted on Law 4990/2022 on 11 November 2022, transposing the EU Whistleblowers Directive into Greek legislation.

PUBLIC SCRUTINY

179. Greece ranks lowest of all EU countries in the World Press Freedom Index 2022, 108th out of 180[284]. In 2021, journalist Giorgos Karaivaz was murdered. The murder has still not been resolved. Journalists face intimidation and Strategic Lawsuits against Public Participation (SLAPPs). Grigoris Dimitriadis[285] launched SLAPPs against news outlets Reporters United and *Efimerida ton Syntakton* (EfSyn)[286] after he was forced to resign. Government Minister Oikonomou sought to discredit a *Politico* reporter, Nektaria Stamouli, by implying that her articles about the spyware scandal were politically motivated[287]. Indeed, two targets of surveillance, Koukakis and Malichoudis, had been reporting in a critical manner about corruption and fraud cases, and the ill treatment of migrants. Athanasios Telloglou and Eliza Triantafillou reported about the spyware scandal, and they were allegedly put under surveillance[288]. In addition, Greece's Supreme Court Prosecutor Isidoros Dogiakos discredited media outlets that criticised the Greek judicial authorities for not handling the Greek wiretapping scandal adequately. He even attempted to intimidate the media investigating the scandal by requesting selective tax audits for their owners[289].

REDRESS

*THE NATIONAL TRANSPARENCY AUTHORITY*

180. As stipulated in Article 82 of Law 4622/2019, the National Transparency Authority (EAD) has the responsibility to strengthen the accountability, transparency and integrity of actions undertaken by government bodies, state bodies, administrative authorities and public organisations. In addition, the EAD ought to prevent, detect and address actions of fraud and corruption by public and private bodies. According to this law, the EAD has taken over all responsibilities, rights and obligations from the following public bodies: the General Secretariat for the Fight against Corruption; the Body of Auditors-Inspectors of Public Administration; the Office of the Inspector General of Public Administration; the Body of Inspectors of Health and Welfare Services; the Body of Inspectors of Public Works; and the Body of Inspectors-Auditors of Transport[290]. While the ADAE's independence is stipulated in the constitution, the EAD is not an independent authority.

---

[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/.
[290] https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019.

181. On 22 July 2022, the EAD started an inquiry into the alleged purchase of the Predator spyware by the Ministry of Citizen Protection and the EYP. The audit checked the Hellenic Police, the EYP and the companies Intellexa and Krikel. The EAD concluded its report on 10 July 2022, but it gave the report to the EYP for prior approval. The official report that was sent to Koukakis on 22 July included only fractions of the full audit as carried out by the EAD. Under the guise of personal data protection, several names in the audit were redacted, including the names of the auditors of the EAD, the EYP prosecutor checking the initial EAD report and the lawyers and accountants of the legal persons involved[291].

182. In the end, the EAD report concluded that both the EYP and the Ministry of Citizen Protection had not concluded contracts with Intellexa and other related national companies. They also had not purchased or used the Predator spyware[292]. However, the EAD did not investigate the bank accounts of Intellexa and Krikel, or those of the affiliated offshore companies. In addition, the EAD only visited the offices of Intellexa and Krikel until two months had elapsed since the first publication about the use of Predator in Greece, at which point employees were working at home owing to COVID-19. The EAD, furthermore, did not meet with legal representatives of the companies in question[293].

183. There are question marks over the independence of the EAD leadership. The current Director, a former employee of Mitsotakis, has held the position ad interim since summer 2022. It is unclear why the recruitment procedure has not been launched. The Director of EAD did not meet with PEGA during the mission in November 2022. The Director did meet with the delegation of the LIBE Committee on 7 March 2023, where questions were raised about spyware in Greece.

*HELLENIC AUTHORITY FOR COMMUNICATION SECURITY AND PRIVACY (ADAE)*

184. In July 2022, Nikos Androulakis confirmed that he had lodged a complaint with the Prosecutor's Office of the Supreme Court that he was allegedly targeted with the Predator spyware on 21 September 2021. Following Androulakis' complaint the ADAE launched an inquiry in August 2022, starting with obtaining information from Androulakis' telecom operator.

185. Predator spyware leaves few traces of infection at the telecommunications providers. However, the ADAE found that Androulakis' mobile phone was monitored by the EYP[294], and that its in-house prosecutor Vasiliki Vlachou had authorised the monitoring action and the lifting of secrecy in September 2021, coinciding with the alleged Predator attack.

186. Following the findings of the ADAE inquiry, Grigoris Dimitriadis and Panagiotis Kontoleon resigned from their government positions[295]. Kontoleon stated that the monitoring of Androulakis was launched at the request of foreign authorities – more

[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'.
[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'.

specifically the Intelligence agencies of Armenia and Ukraine – in the light of Androulakis' participation in the European Parliament Committee on International Trade, which deals with trade relations between the EU and China[296]. Both Ukraine and Armenia have repudiated these claims[297].

187. On 15 December 2022, the authority followed up on requests from journalists Tasos Telloglou and MEP Giorgos Kyrtsos on whether they had been targeted by the EYP. An audit by the ADAE into the telecommunications company Cosmote found that both Telloglou and Kyrtsos were indeed under surveillance[298]. Cosmote informed the Supreme Court and questioned the legality of the ADAE's investigation[299]. The ADAE set up a special team to scrutinise the telecommunications providers, specifically looking for further requests made by the EYP for the lifting of confidentiality[300].

188. The government has attempted to replace the members of the ADAE's Board of Directors. In addition, Greece's Chief Prosecutor Dogiakos officially issued an opinion on 10 January 2023, ruling that the ADAE cannot conduct investigations into the records of telecommunications providers to look into the lifting of the confidentiality of communications. According to the opinion, criminal sanctions could apply once the ADAE starts such audits[301]. This opinion, which contradicts previous opinions of the Attorney General, clearly violates the independence of the ADAE[302] and attempts to prevent it from conducting investigations. During a PEGA Committee meeting on 28 February 2023, Rammos stated that Dogiakos' opinion is not binding and the tasks of the ADAE can carry on as usual[303].

189. The ADAE has confirmed that the EYP has also spied on the head of the Greek armed forces, Konstantinos Floros, a serving minister, several officers that deal with arms cases and a former national security advisor. Owing to the current inability of the ADAE to inform the target persons, the ADAE intended to present the findings to the Greek Parliament's transparency committee and the Greek Parliament's institutions[304]. Christos Rammos sent a letter to the Greek Parliament asking for this presentation. Initially, the President avoided raising the issue for discussion by saying that he had not found time to read Rammos' letter during his name day. Eventually, the Néa Dimokratía majority within the Committee on Institutions and Transparency denied his request. On 24 January 2023, the Spokesperson of the Government attacked the ADAE and its

[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"'.
[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] PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos, 28 February 2023.
[304]https://www.protothema.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/.

president for its investigations[305], arguing that Rammos was performing 'activism' and 'overstepping' his mandate, which did not help the investigations conducted by the ADAE. On 25 January 2023, SYRIZA leader Alexis Tsipras publicly named those listed in the report at the Greek Parliament, confirming that the Head of the Armed Forces, the former head of the Greek Army, the Minister of Labour, the former PM's National Security Advisor, as well as two advisors from the Directorate of Equipment of the Armed Forces, were under surveillance by the EYP. Given the seriousness of the findings, the refusal to allow the ADAE to report to the Greek Parliament and the discrediting of the authority amount to the obstruction of accountability and transparency[306].

190. In addition, Rammos stated that the changes to the legal framework of the ADAE have created uncertainty, resulting in an exchange of letters with the ministries in order to clarify the authority's operational framework for complaints and investigations. Rammos mentioned that the ADAE receives approximately 10 complaints per day[307].

*COMMITTEE ON INSTITUTIONS AND TRANSPARENCY*

191. In July 2022, the Committee on Institutions and Transparency summoned Kontoleon and the president of the ADAE Christos Rammos to a parliamentary hearing. During this hearing, Kontoleon reportedly admitted that the EYP had spied on Thanasis Koukakis for national security reasons, but stated that he had no knowledge of the attempted Predator hack of Androulakis' device. Giannis Oikonomou – government spokesperson – reported that the Greek authorities have neither acquired nor used the Predator spyware[308].

192. Although the meetings are in camera[309], reportedly neither Kontoleon nor Dimitriadis were willing to provide substantial evidence, invoking national secrecy reasons[310]. The new head of the EYP, Demiris, denied the committee access to a report containing information on the alleged destruction of surveillance data[311]. This effectively means that the EYP refuses accountability and the Greek Parliament cannot carry out its mandate of parliamentary oversight.

193. On 30 August 2022, the committee summoned nine people for a behind-closed-doors hearing, including public prosecutor Vasiliki Vlachou, former Secretary-General Grigoris Dimitriadis and former head of the EYP Kontoleon. All of them invoked

[305] https://www.protothema.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'.
[307]PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos, 28 February 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'.

confidentiality and avoided answering questions during this committee hearing[312].

*PARLIAMENTARY COMMITTEE OF INQUIRY*

194. A proposal by the PASOK-KINAL party to set up a committee of inquiry into the alleged use of spyware[313] was endorsed by 142 opposition MPs, while the 157 Nea Demokratia MPs abstained[314]. However, ND had an absolute majority in the committee of inquiry. The calls for a bipartisan Bureau were rejected. ND determined the work programme and list of witnesses to be invited, and rejected several of the witnesses proposed by the opposition parties. The committee was established on 29 August 2022. It began its work on 7 September 2022 and concluded its work on 10 October 2022.

195. The government majority in the committee refused to invite Mr Bitzios and Mr Lavranos, but it did invite Stamatis Tribalis - current manager of Krikel - and Sara Hamou. On 22 September, Tribalis testified in front of this parliamentary committee. Mr Tribalis presented blatantly false information about the involvement of Bitzios and Lavranos in Krikel, claiming, among other things, that he was the owner of Krikel[315].

196. One witness, Sarah Hamou of Intellexa, claimed to be unable to appear in person (although she lives in Cyprus), and she was allowed to submit answers in writing. Common conclusions could not be reached due to severe polarisation of the political landscape. A government-led majority decided to classify some 5 500 pages of documents, including the minutes and the deposition of Hamou and the main findings of the parties, although it is entirely within the powers of Parliament to declassify and provide access to this information. Therefore, no public summary was prepared. Only the final debate in the Plenary of the Greek Parliament was public and the findings of both PASOK and SYRIZA were published by the parties themselves.

197. The opposition proposed other witnesses, such as Koukakis, Mitsotakis, Dimitriadis, Vlachou, Lavranos and Bitzios, but the committee eventually declined to invite them. On 10 October 2022, the committee finished its investigations and the different political parties all submitted their final reports[316].

*HELLENIC DATA PROTECTION AUTHORITY*

198. The Hellenic Data Protection Authority (HDPA) is an independent authority and has the role of supervising the application of the General Data Protection Regulation[317] (GDPR), other regulations and national laws concerning data protection of the individual in Greece[318]. The 4624/2019 law excluded national security from the remit of

---

[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.*
[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] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).
[318] Hellenic Data Protection Authority. *Personal data*.

the HDPA, while it had been included since the law of 1997[319]. Following the complaint by Nikos Androulakis in July 2022, the authority started an inquiry in July 2022 into the installation of spyware on mobile phones and the personal data collection and data processing that followed. The authority conducted an audit at the Intellexa office in Chalandri and at an Intellexa establishment in Elliniko. However, Intellexa failed to provide crucial information and answered the questionnaires after a considerable delay, thus obstructing the audit of the authority[320].

199. On 16 January 2023, the HDPA fined Intellexa S.A. EUR 50 000[321] for its obstruction and its unwillingness to cooperate during the audit on the basis of Article 31 of the GDPR.

200. Following the action taken by the HDPA, Intellexa has handed over documents but the authority is still looking into them. According to President of the HDPA, Mr Menoudakos, the authority did discover domain names that possibly belong to companies cooperating with Intellexa within and outside the EU. The HDPA's investigation is still ongoing[322].

201. During a PEGA Committee meeting on 28 February 2023, the president of the HDPA mentioned that an HDPA inquiry looked into internet applications for sending text messages. According to Mr Menoudakos, companies have made use of these internet applications to deliver text messages related to the Predator spyware. The HDPA is currently trying to identify the targets but has so far confirmed that 300 text messages have been sent to approximately 100 receivers using this method. The HDPA has instructed the companies to preserve this data and underlined that if these companies have no legal representative in the EU they are violating the GDPR[323].

THE TARGETS

*THANASIS KOUKAKIS*

202. In the summer of 2020, journalist Thanasis Koukakis was wiretapped by the EYP. During that time, he was reporting on financial topics, including the Piraeus/Libra scandal, involving Felix Bitzios, and alleged tax evasion by Greek businessman Yiannis Lavranos, and on controversial banking laws introduced by the Greek government impeding the prosecution of money laundering and other financial wrongdoing (indeed the retroactive effect led to 12 pending cases being dropped)[324]. Mr Koukakis was also investigating the procurement for new ID cards, where Mr Lavranos and Mr Bitzios had a business interest. Around the time of Mr Koukakis's first appearance before PEGA, the tender was suddenly withdrawn and the General Secretary responsible resigned.

203. On 29 July 2022 EYP chief, Panagiotis Kontoleon declared that the EYP had monitored

[319] Government Gazette of the Hellenic Republic.
[320] Hellenic Data Protection Authority. Imposition of a fine on Intellexa S.A. for non-cooperation with the HDPA.
[321] Hellenic Data Protection Authority. Imposition of a fine on Intellexa S.A. for non-cooperation with the HDPA.
[322] PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.
[323] PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.
[324] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis*?.

Mr Koukakis's phone for 'national security reasons'.

204. On 1 June 2020, the EYP submitted a first request to lift the confidentiality of Mr Koukakis's telephone number for two months, until 1 August 2020. EYP submitted a request for an extension of an additional two months[325], i.e. until 1 October 2020. The Prosecutor of the Court of Appeals - Vasiliki Vlachou - has approved all these provisions on the grounds of national security[326].

205. However, 12 days later, on 12 August 2020, the EYP suddenly requested the termination of the lifting of the confidentiality of Mr Koukakis's telephone number, i.e. a month and a half earlier than foreseen in the original request. That happened on the same day as when Koukakis approached ADAE with the request to be informed about the possible monitoring of his two mobile phones and a landline.

206. On 10 March 2021, the ADAE reported to the Prosecutor of the EYP on the possibility of notifying Koukakis about the surveillance of his mobile phone. However, on 31 March, the Greek government passed Amendment 826/145 depriving the ADAE of the ability to notify citizens of the lifting of the confidentiality of communications with retroactive effect[327]. The president of the ADAE, Christos Rammos, and two other members of the ADAE have argued against this amendment, pointing out in an op-ed that the amendment violates the right to respect for private and family life enshrined in the European Convention on Human Rights (ECHR) and the protection of confidentiality of communications as guaranteed in the Constitution[328].

207. Between 12 July 2021 and 14 September 2021 Mr Koukakis's telephone was infected with Predator spyware[329]. According to Mr Koukakis, he received a text message with a link to a financial news webpage[330]. On 28 March 2022, Citizen Lab officially revealed the infection[331].

208. Mr Koukakis made several attempts to obtain redress for the surveillance attempts. He filed two complaints with the ADAE: the first on 6 April 2022 where he requested a thorough inquiry into the Predator infection of his mobile phone; the second on 13 May 2022 in the light of the new revelations published by InsideStory and Reporters United. In addition, Mr Koukakis filed a complaint with the EAD on 4 May 2022, in which he requested an investigation into the background of the interceptions by the EYP and the Predator attack[332].

---

[325] Reporters 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] European Parliament. Hearing 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. The investigation by the National Transparency Authority (EAD) on 21 July 2022 into the Athens offices of Intellexa, the vendor of Predator spyware, was limited and superficial, despite the fact that vital information on the Predator attacks - a criminal offence - could have been found. No servers, IT hardware or administration were seized and secured. The verification of the financial administration was limited to the year 2020[333]. The Cyprus and Ireland subsidiaries of Intellexa were not investigated at all[334]. The investigations did not include information on the bank accounts of Intellexa and subsidiaries[335]. Mr Koukakis appealed to the European Court of Human Rights on 27 July 2022[336].

210. On 5 October 2022, Mr Koukakis filed a complaint with prosecutors in Athens against Intellexa Alliance, and particularly Tal Dilian and Sara Hamou[337], for violating the confidentiality of his communications[338].

*NIKOS ANDROULAKIS*

211. On 21 September 2021 Nikos Androulakis, leader of the centre-left PASOK-KINAL and Member of European Parliament was targeted with the Predator spyware when a malicious link was sent to his telephone[339]. Mr Androulakis received a text message stating 'Let's get a little serious, man, we've got a lot to gain'. In addition, the message included a link to install the Predator spyware on his phone but, unlike Mr Koukakis, Mr Androulakis did not click on the link that was sent to him[340]. During a PEGA Committee meeting on 28 February 2023, Mr Androulakis stated that the HDPA identified the credit card account that paid for the text messages sent to him. This information was shared with the relevant prosecutor[341].

212. In July 2021, Mr Androulakis announced his candidacy in the race for party leadership[342]. According to the ADAE inquiry, Mr Androulakis's mobile phone was at that time being monitored by the EYP through the telecommunications providers[343]. EYP Prosecutor Vasiliki Vlachou approved the lifting of secrecy of Mr Androulakis's phone on 'national security' grounds. The approval coincided with both the Predator targeting and Mr Androulakis's candidacy.

213. When Mr Androulakis was elected party leader in December 2021, the 'official' EYP monitoring was terminated abruptly[344], despite the fact that the two-month re-authorisation for his surveillance had not yet expired.

214. On 28 June 2022, DG ITEC of the European Parliament checked Mr Androulakis's

---

[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] PEGA Committee Exchange of Views with Konstantinos Menoudakos and 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*.
[344] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader*.

phone and found the evidence of the attempted Predator hack of September 2021, and informed Mr Androulakis accordingly[345]. Mr Androulakis filed a criminal report to the prosecutor's office of the Supreme Court on 26 July 2022[346].

215. A few days later, on 29 July, Mr Androulakis presented the information about the Predator attack to the ADAE. On the same day, the Permanent Committee on Institutions and Transparency heard EYP chief Panagiotis Kontoleon and Christos Rammos, President of the ADAE, in the presence of the Ministers of Digital Governance and State. The meeting took place behind closed doors[347].

216. On 8 September 2022, Mr Androulakis asked the ADAE to hand over his wiretapping files[348]. However, on this same day, Ta Nea reported on an official briefing from the ADAE mentioning that the files of both Mr Androulakis and Mr Koukakis had been destroyed by the EYP[349]. The destruction is an unequivocal fact, but the story behind the destruction remains unclear. On the one hand, some sources blame the destruction of the files on the change in the electronic systems of the EYP in 2021[350]. This change to the new legal assembly system allegedly caused a technical problem resulting in the destruction. On the other hand, other sources claim that Mr Kontoleon gave the order on the 29 July 2022 to destroy these files on the same day that Androulakis informed the ADAE about the surveillance attempts[351]. During a PEGA Committee hearing, President of the ADAE, Mr Rammos, did not confirm nor deny the destruction of records[352].

217. On the 5 August, Mr Kontoleon and Mr Dimitriadis resigned from their positions. On 8 August Mr Mitsotakis made a television statement, acknowledging the wiretapping of Mr Androulakis, but reiterating the fact that he was unaware of the surveillance[353].

218. EYP has so far declined to disclose the reasons for the surveillance. It has offered to inform Mr Androulakis privately of the reasons. This would be unlawful.
Mr Androulakis asked for his surveillance file to be submitted to the Committee on Institutions and Transparency, but that was rejected.

219. On 7 December 2022, Mr Androulakis lodged a complaint with the European Court of Human Rights over his wiretapping by the EYP and the lack of official information about his case[354].

220. Surveillance of a politician is highly unusual, and the Greek Constitution provides for special protection of politicians. The EYP denies any involvement in the surveillance with Predator. The government initially floated suggestions about foreign powers that supposedly requested the wiretapping of Mr Androulakis, or they suggested that his

---

[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. Hearing of 8 September 2022.
[353] Reuters. *Greek PM says he was unaware of phone tapping of opposition party leader.*
[354] Ekathimerini. *Socialist leader appeals to European Court over tapping.*

membership of an EP committee in charge of relations with China might be the reason. None of these hypotheses were very credible. The surveillance occurred in a political context of upcoming elections. PASOK would be the preferred coalition partner. In the autumn of 2021, there were four candidates in the PASOK leadership contest, each with different views on such a coalition. Mr Androulakis was said to be open to the idea, but not under the Premiership of Mr Mitsotakis. Another candidate, Andreas Loverdos, had served earlier as a Minister in a Néa Demokratía - PASOK coalition, and was thought to be more supportive. He was acquainted with Mr Dimitriadis. The publication of the list of other alleged targets by Documento, reinforces the suspicion of political reasons for the surveillance. There is no proof for any of these hypotheses, but it is essential that these avenues are investigated and eliminated where possible.

*GIORGOS KYRTSOS*

221. On 15 December 2022, an ADAE audit into Cosmote telecommunications company confirmed that Member of European Parliament Giorgos Kyrtsos was under surveillance by the EYP[355]. Both his mobile phones and his landline were wiretapped. The surveillance was reportedly prolonged nine times[356] for a period of 18 months.

222. Giorgios Kyrtsos is a former member of Nea Demokratia and of the European People's Party. In February 2022, ND expelled Mr Kyrtsos from the Greek ruling party on account of his disapproval of the government's action surrounding the COVID-19 pandemic, media freedom restraints and the approach to the Novartis scandal[357]. After his expulsion, Mr Kyrtsos joined Renew Europe.

*STAVROS MALICHOUDIS*

223. On 13 November 2021, EFSYN newspaper revealed that several journalists reporting on refugee cases were allegedly being wire-tapped by the EYP. An internal document from EYP showed that the EYP ordered monitoring and collection of data on Greek journalist Stavros Malichoudis[358,359]. Malichoudis was writing about a 12-year-old Syrian child who was forced to live for several months in a detention camp on the Greek island of Kos[360].

224. On 15 November 2021, government spokesperson Giannis Oikonomou indirectly confirmed the claims. He stated that the EYP could wiretap individuals if there is a risk to national security from 'internal or external threats'[361]. However, on 24 November and 17 December 2021, Minister of State George Gerapetritis denied any surveillance of journalists in Greece, including that of Mr Malouchidis, but according to media outlet Solomon he neither confirmed nor denied the authenticity of the EYP internal documents[362].

---

[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 EPP.*
[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.

225. During the PEGA hearing on Greece on 8 September 2022, Mr Malichoudis stated that through wiretapping his phone, the EYP could also collect information from colleagues and journalists that he was in contact with during that time[363]. The EYP could have allegedly listened in on conversations Mr Malichoudis had with the International Organisation for Migration (IOM)[364], pointing out the danger to other people of the 'by-catch' from wiretapping an individual. In addition, during the hearing Mr Malichoudis showed evidence that the EYP was interested in his work and sources, but that the reason for the monitoring is covered by 'national security'[365].

*CHRISTOS SPIRTZIS*

226. On 9 September 2022, former Minister of Infrastructure and lawmaker for the Syriza party Christos Spirtzis claimed to have been targeted with the Predator spyware on his mobile phone[366]. Spirtzis had submitted critical parliamentary questions to the government on the surveillance tasks of the EYP on 15 November 2021. That same day he received a similar message[367] as the one Nikos Androulakis had received. On 19 November, a second message was sent to Christos Spirtzis containing a link to an article of Efimerida ton Syntakton[368]. While CitizenLab did not check these messages, Spirtzis did share the links he received with two technicians who verbally confirmed that he had been targeted[369]. On 9 September 2022, Spirtzis lodged a complaint with the prosecutor of the Supreme Court[370]. Spirtzis is a confidante of party leader Alexis Tsipras, and present during high-level meetings of the party leadership.

*TASOS TELLOGLOU, ELIZA TRIANTAFYLLOU AND THODORIS CHONDROGIANNOS*

227. Journalists Tasos Telloglou and Eliza Triantafylou have allegedly been spied upon during their investigative work for the new outlet Inside Story. In an article for the Heinrich-Böll-Stiftung on 24 October 2022, Telloglou shared his surveillance and intimidation experiences while investigating the surveillance scandals in Greece. According to these experiences, he believes he was monitored between May and August 2022[371].

228. In addition, a source from the security services had told Telloglou in June 2022 that the locations of he and his colleagues Eliza Triantafyllou (InsideStory) and Thodoris Chondrogiannos (Reporters United) were monitored by the authorities to assess what sources they were meeting[372]. At time of writing, the Greek government has not yet responded to the allegations.

---

[363] European Parliament. Hearing of 8 September 2022.
[364] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*
[365] European Parliament. Hearing of 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.*
[369] Inside story, *Predator: More than 20 targets in Greece according to the Data Protection Authority.*
[370] Reuters. *One more Greek lawmaker files complaint over attempted phone hacking; Euractiv. Another Greek opposition lawmaker victim of Predator.*
[371] Heinrich-Böll-Stiftung. *A State of Absolute Solitude.*
[372] MapMF, *Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations.*

229. On 15 December 2022, an ADAE audit of Cosmote telecommunications company confirmed that Telloglou was under surveillance by the EYP. Owing to 'national security', the reasons for the surveillance were not revealed[373].

OTHER TARGETS

230. On 29 October 2022 reported that other politicians had been targeted with the Predator spyware, including a government minister who was not on good terms with the prime minister. In addition, another member of Néa Demokratía reportedly received a link to instal Predator[374]. A government spokesperson, Mr Oikonomou stated that the article lacks concrete evidence[375].

231. On 5 and 6 November 2022 Documento reported on a list containing 33 names of persons targeted with Predator spyware[376]. The list included many high-profile politicians, including members of the current government, former Prime Minister Samaras, former EU Commissioner Avramopoulos, the editor in chief of a national government-friendly newspaper, and persons in the entourage of Vangelis Marinakis, ship-owner, media mogul and owner of football clubs Olympiakos and Nottingham Forest. The ADAE confirmed that some names on the list were monitored by the EYP through conventional wiretapping. These names include MEP Giorgos Kyrtsos[377], Chief of Joint Staffs General Konstantinos Floros[378], Chief of the Hellenic Army Haralambos Lalousis[379], Minister of Labour and Social Affairs Kostis Hatzidakis[380], former General Directors of Defence Equipment and Investments Theodoros Lagios and Aristides Alexopoulos[381], former security advisor Alexandros Diakopoulos[382] and Greek investigative journalist Tasos Telloglou[383].

232. In addition, Meta's former Cybersecurity Policy Manager Artemis Seaford also appeared on the list of 33 names and was confirmed to be simultaneously wiretapped by the EYP and spied upon with Predator. Seaford was wiretapped by the EYP from July 2021 until the summer of 2022, meaning that the authorisation for wiretapping Ms Seaford's device was renewed six times, all of which in principle require approval from the EYP's in-house prosecutor Vasiliki Vlachou. CitizenLab confirmed that her mobile phone was also infected with Predator for at least two months as of September 2021. The Predator infection thus happened approximately one to two months after the conventional wiretapping started. Ms Seaford stated that information on her COVID-19

---

373 Euractiv, Another MEP and journalist the latest victims of 'Greek Watergate'.
374 Ta Nea, *Four illegal manipulations by suspicious center.*
375 Politico, *Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.*
376 Documento, 6 November 2022.
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/*.

vaccine appointment was obtained from her text messages via conventional wiretapping. This information was subsequently used to create a sophisticated automated SMS, using the same outline as the official appointment, with the request to confirm the appointment via a link. Clicking on this link infected the device with Predator spyware. The SMS messages contained accurate and detailed information of her vaccination file, and it was sent just minutes apart from the real, official, messages, indicating that whoever sent the messages had access to the content and timing of the SMS messages, whichEYP would have had through the conventional wiretap.

233. Wiretapping and/or surveillance of a private individual is unusual, especially when national security cannot be legitimately invoked in such a case. This begs the question what other motives could have played a role in the targeting. The surveillance occurred while Ms Seaford was working at Meta, a company that has published a threat-report on the surveillance-for-hire industry and banned multiple spyware companies, including Cytrox, from its platform. It is, however, highly unlikely that her role at Meta was the reason for the surveillance. The Meta threat-report was only published in December 2021, few months later than the timing of the targeting of Ms Seaford's device, and none of the other people involved in writing the report were themselves targeted. In addition, Ms Seaford stated[384] that she was only partly involved in these activities and that Meta is very discreet about communicating the names of its employees.

234. In March 2021, magazine Marie-Claire published an article including an extract from a book series written by Ms Seaford. The article mentions Seaford's experiences with everyday sexism and harassment in Greece and it particularly describes a case of sexual harassment by 'a politician'[385]. The surveillance started a few months later. One explanation may be that the politician in question read the article and feared his name might be publicly disclosed. Another explanation could be that someone else recognised the politician from the description in the article, and wanted to gather more information on that person, for political reasons. Whichever the case may be, only very few persons would have the power to both submit an official request for wiretapping to the EYP, and to arrange for Predator spyware to be used. The combination of surveillance by the EYP and Predator spyware has been confirmed in other cases as well.

235. It isimportant that these possibilities be further investigated, in particular the question of who requested the surveillance by the EYP. Ms Seaford has filed a request with the ADAE and has lodged a complaint with the court in Greece. However, the investigation is still under way. She is the first American citizen known to have been targeted in the EU[386][387].

236. Other names on the list that were not officially confirmed are Former Minister for Education and Religious Affairs Andreas Loverdos, former Prime Minister Antonis

[384] PEGA Committee Meeting, 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] PEGA Committee Meeting, 20 April 2023.

Samaras, Minister of State George Gerapetritis, Former Commissioner Dimitris Avramopoulos, Minister Nikos Dendias, Minister of Education Niki Kerameus, Minister Akis Skertsos, Minister of Investment Nikos Papathanasis, former Minister of Citizen Protection Mihalis Chrysochoidis, Deputy Defence Minister of the Hellenic Republic Nikos Hardalias, Aristotelia Peloni, MP Christos Spirtzis, former Minister of Citizens' Protection Olga Gerovasili, Head of the Hellenic Police Michalis Karamalakis, head of the Economic Prosecutor's Office Christos Barkadis, EYP's in-house Prosecutor Eleni Vlachou, Government Spokesman Giannis Oikonomou, EYP's Deputy Chief Vassilis Grizis; the revelations on the list are highly disturbing not just because of the high-profile names but also because the abuse of spyware is systematic, and large-scale.

237. In 2023 the ADAE reported that the EYP has also wiretapped a serving minister, several officers that dealt with arms cases and a former national security advisor[388].

CONCLUDING REMARKS

238. There are patterns suggesting that the Greek government enables the use of spyware against journalists, politicians and businesspersons. It also allows the export of spyware to countries with poor human rights records and provides a training centre for non-EU country agents that want to learn about spyware. Although the use of spyware is illegal in Greece, the investigation into origins of the spyware attacks only gained momentum in Summer 2022. A political majority is reportedly being used for the advancement of particular interests rather than the general interest, in particular by the appointment of associates and loyalists in key positions such as the EYP, EAD (National Transparency Authority) and Krikel (a company specialised in electronic security systems). The highest political leadership in the country use spyware as a tool for political power and control, in some cases in parallel or after legal interception. Greece has a fairly robust legal framework in principle. However, legal amendments have weakened crucial safeguards, and political appointments to key positions are an obstacle to scrutiny and accountability. *Ex ante* and *ex post* scrutiny mechanisms have been deliberately weakened, and transparency and accountability are evaded. Critical journalists or officials fighting corruption and fraud face intimidation and obstruction. Overall the system of safeguards and oversight of surveillance is inadequate for the protection of citizens against abuse by state agencies and private actors. More needs to be done to address this problem. In addition, the pretext of 'national security' is invoked as justification for the wiretapping of individuals.

239. Spying for political reasons is not new to Greece, but the new spyware technologies make illegitimate surveillance much easier, in particular in a context of severely weakened safeguards. Unlike other cases, such as Poland, the abuse of spyware does not seem to be part of an integrated authoritarian strategy, but rather a tool used on an ad hoc basis for political and financial gain. However, it erodes democracy and the rule of law just as much, and leaves ample room for corruption, when these turbulent times call for reliable and responsible leadership.

*I.D. Cyprus*

[388] Politico. *Brussels Playbook: Globalization's sanatorium - Vestager rings alarm - S(upended & D(dumped).*

240. The Committee visited Cyprus in November 2022 as part of a joint mission to Greece and Cyprus. Members met the Minister for Energy, Commerce and Industry, other government officials and members of the House of Representatives sitting on relevant committees to discuss the current legal framework for spyware. They also heard from legal experts, NGO representatives and journalists who submitted documentation on surveillance and corruption to the Committee. The Committee stressed that more should be done on beneficial ownership registries, which lack transparency although they were designed to shed light on such issues.

241. In contrast to other Member States, there is not much information on the use of spyware by Cyprus. There are no officially confirmed cases of persons that are or were illegally targeted with spyware. However, journalist Makarios Drousiotis was allegedly monitored using both eavesdropping techniques and spyware by the Cypriot government in February 2018[389]. On paper, there is a robust legal framework, including EU rules, but in practice, Cyprus is an attractive place for companies selling surveillance technologies. The government however denies this and points to a decline in registered spyware companies in the country. Recent scandals have damaged the reputation of the country though and a set of new legislative initiatives tightening the legal framework for exports and improving compliance is expected to be finalised in 2023.

242. There are close connections between Cyprus and Greece on spyware. Tal Dilian's Intellexa is established in Greece and his Predator spyware was used in the Greek hacking scandals. Both countries were also involved in the illegal export of Predator spyware to the Sudanese Rapid Support Forces (RSF) militias[390]. Greece issued an export licence, whereas the material was shipped to Sudan from Larnaca airport[391].

243. In addition to the export of spyware outside the EU, Cyprus also facilitates the trade in subsystems and spyware technology to Member States. The name of UTX Technologies - registered in Cyprus and acquired by the Israeli technology giant Verint - has been spotted on invoices of German, French and Polish companies that shipped Gi2 technology and monitoring systems[392].

244. On paper, there is a legal framework in place stipulating the protection of private communications, the processing of personal data and the individual’s right to information. However, in practice, once national security is invoked, there are no clear-cut rules regulating the use of interception devices and the protection of citizens’ constitutional rights.

LEGAL FRAMEWORK

*THE DUAL-USE REGULATION*

245. Cyprus seems to collaborate very closely with Israel on surveillance technologies. Cyprus consulted Israel and the US about the reform of its legal framework and system

[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).

of control of exports of dual-use items. Cyprus is a popular destination for many Israeli spyware companies.

246. The Ministry of Energy, Commerce and Industry in the Strategic Items Export Licensing Section regulates the export of dual-use items[393]. In response to the PEGA questionnaire that was sent to all Member States, Cyprus stated that it monitors and assesses all export licence applications for dual-use goods on a case-by-case basis, in full compliance with relevant sanctions regimes. These regimes are the European Union Global Human Rights Sanctions Regime as well as the EU Dual-Use Regulation, guided by the criteria of the relevant Council Common Position (2008/944/CFSP)[394]. The PEGA committee observes that Cyprus is not a participant in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. It has been stated that Turkey blocked Cypriot participation in the Arrangement during the PEGA Committee mission. However, the government declares it is adhering to the same standards.

247. The Ministry of Energy, Commerce and Industry can consult the so-called Advisory Committee about the granting of export licences. This Committee consists of representatives from the Ministry of Defence, Ministry of Justice and Public Order, Ministry of Foreign Affairs and the Customs and Excise Department among other departments[395]. According to the Cypriot government, this Committee is regularly consulted when export applications are examined. On several occasions, the export of dual-use goods to third countries has been rejected following a negative opinion from this committee[396]. The Chamber of Commerce usually does not provide information on the number of approved and rejected software-marketing licenses[397].

248. During the PEGA Committee's mission to Cyprus on 1 and 2 November 2022, the participants on the mission had a meeting with the Ministry for Energy, Commerce and Industry and the Deputy Minister for Research, Innovation and Digital Policy. Ministers Natasa Pilides and Kyriacos Kokkinos stated that there had been a sharp decline in the number of companies active in spyware in Cyprus. 32 companies were registered, but according to the Minister at the time of the visit only 8 to 10 were active, with three or four producing spyware[398]. However, they also acknowledged technical challenges in overseeing and controlling companies based in Cyprus selling individual spyware components independently.

249. In practice, Cyprus is reportedly rather lenient about providing spyware companies with export licences[399]. Companies use techniques to circumvent the rules: the physical product hardware is sent to a recipient country without the software loaded on it[400]. After that, the activation software (also referred to as the 'licence key') is sent

[393] http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument.
[394] Reply to the European Parliament questionnaire received from Cyprus.
[395] Lelaw, 'Export Controls for dual-use products'.
[396] Reply to European Parliament questionnaire received from Cyprus.
[397] Inside Story, 'Who signs the exports of spyware from Greece and Cyprus?'.
[398] Meeting with Ms Natasa Pilides, Minister for Energy, Commerce and Industry and Kyriacos Kokkinos, Deputy Minister for Research, Innovation and Digital Policy during PEGA mission on 2 February 2022.
[399] InsideStory, 'Who signs the exports of spyware from Greece and Cyprus?'.
[400] InsideStory, 'Who signs the exports of spyware from Greece and Cyprus?'.

separately on a USB memory stick to the destination country[401]. Another way is to state that the product is exported for demonstration purposes only, although a detailed description of the product is included[402]. In addition, unclear descriptions of the spyware are filled in in the export form for export licences, which has hindered appropriate custom checks.

250. Several Cypriot companies have reportedly obtained export licences for the sale of 'dual-use items' to non-EU countries. These companies are UTX Technologies, Coralco Tech, Prelysis and Passitora[403].

251. UTX Technologies has been involved in the sale of spyware to EU Member States as well as to non-EU countries. Between 2013 and 2014, UTX has been mentioned on invoices to German (Syborg Informationsysteme), French (COFREXPORT) and Polish (Verint) companies for the trade in monitoring systems and Gi2 technology[404].

252. The Cypriot Trade Service has provided temporary export licenses to Cognyte subsidiary UTX Technologies for the sale of surveillance software to Mexico, United Arab Emirates, Nigeria, Israel, Peru, Colombia, Brazil and South Korea[405]. UTX Technologies reportedly also had a contract with Thailand for the sale of surveillance subsystems for USD 3 million. The description of these subsystems made reference to a 'dual-use' type with 'speech analysis algorithm' and 'metadata and voice'. The agreement also contained a specific reference to a Lithuanian company. As the Cypriot authorities would not issue the export licence, the Ministry of Energy, Commerce and Industry could be circumvented through the Lithuanian registered UAB Communication Technologies[406]. Russian-Israeli citizen Anatoly Hurgin owns this company and in addition holds a Maltese passport[407]. In addition, UTX also secured an agreement with Bangladesh for a web intelligence system for USD 2 million in 2019 and for a cellular tracking system for USD 500 000 in 2021[408].

253. Cyprus's export history also shows that Coralco Tech - originally from Singapore but also registered in Israel and Nicosia - shipped monitoring equipment for USD 1.6 million to the Bangladeshi military after a tender process in 2018. The owner of Coralco Tech is the Israeli Eyal Almog[409].

254. In 2019, the internal intelligence agency of Bangladesh (NSI) bought Wi-Fi interception software from Prelysis (registered in Cyprus) for a total of USD 3 million. Kobi Naveh - the founder and director of Prelysis - worked for the Israeli company Verint until 2014. Verint is also the company that acquired the Cyprus-registered UTX Technologies[410].

---

[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/.
[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'.

255. In summer 2021, Bangladesh additionally bought a spy vehicle from Tal Dilian's firm Passitora (formerly WiSpear). The Swiss company Toru Group Limited, registered in the British Virgin Islands, served as an intermediary for the agreements made with Dilian's Passitora[411].

256. On 4 October 2022, it was revealed that in November 2019 the Dutch Ministry of Defence had been about to sign an agreement with WiSpear, the company owned by Tal Dilian, which had earlier acquired Cytrox, the manufacturer of Predator spyware[412]. According to media reports and statements made by the DISY (Dimokratikós Sinagermós) President, WiSpear sent an email to the governing party DISY and the Ministry of Energy, Trade and Industry asking for assistance in implementing the agreement with the Dutch Defence Ministry[413]. It is not clear whether the contract was signed and any spyware was provided to the Dutch Defence Ministry.

257. These examples show there is a lot of surveillance industry activity in Cyprus involving the same actors that emerge in the spyware scandal that is being investigated by PEGA.

258. Many Israeli companies come to Cyprus to start their European activity[414]. Furthermore, different sources have reported that the country is home to approximately 29 Israeli companies[415]. Some sources point to a close connection between the trade in spyware and diplomatic relations. In return for the facilitation of licences for Israeli companies, Cyprus has allegedly received some of the products these companies develop and export, such as the Pegasus spyware from NSO[416] as well as spyware materials from WiSpear[417]. Cyprus serves as the foothold for the trade in Israeli spyware within the EU's internal market as well as for the export of spyware to non-EU countries.

*EX ANTE* SCRUTINY

259. The law on the Protection of the Confidentiality of Private Communications 92(I)/1996 stipulates that the Attorney General may submit an application to the Court for the issuance of a judicial warrant that authorises or extends the interception of private communications by an authorised person. This application by the Attorney General to the Court requires a written request by the Chief of Police, the Commander of the Cyprus Intelligence Service or an investigating judge. Provisions on the authorisation or approval can however be overruled in cases where the interception of private communication is in the security interests of Cyprus or to prevent, investigate or prosecute offences[418].

260. After the application, the Chief of Police - in agreement with the Deputy Chief of Police and the Commander of the Cyprus Intelligence Service - provides a written

[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. Chapter 6. Published 2022.
[416] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 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).

authorisation to employees of their service or employees carrying out assignments for their service to intercept private communications and/or obtain access to the monitoring equipment for the purposes of technical work[419].

261. In addition, Article 4(2) of Law 92(I)/1996 as amended in 2020[420], stipulates that if a device or machine has been primarily designed, produced, adapted or manufactured in order to allow or facilitate the interception or monitoring of private communication, no person is allowed to import, manufacture, advertise, sell or otherwise distribute such devices or machines. Violation of this article can lead to a fine of EUR 50 000 euro and/or up to five years' imprisonment[421]. These provisions do not apply if the provider has informed the Central Intelligence Service (KYP), the Police and the Commissioner and secured their approval. These provisions do not apply to the surveillance systems used by the Chief of the Police and the Commander of the KYP[422].

*EX POST* SCRUTINY

262. In Cyprus, the Law Providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 provides that if personal data is used or if an individual has been the subject of processing, the individual in question has the right to be informed[423]. This right can be circumvented once the Commissioner for the Protection of Personal Data decides otherwise in light of national security reasons among others[424].

263. Moreover, the Protection of the Confidentiality of Private Communication Law adopted in 1996 specifies that in case of interception of private communications by law enforcement agencies, the Attorney General is obliged to inform the individual in question. The individual must be notified within a maximum period of 90 days from the start date of the judicial warrant[425] or within a maximum period of 30 days as of the execution of this judicial warrant. The Attorney General must provide the individual in question with a report detailing the issuance of the court warrant, the date of issuance of the court warrant and the fact that within this period, interception or access to private communications has occurred. This obligation can be temporarily suspended if the Attorney General decides that withholding this information is in the interest of the security of Cyprus, among other reasons[426]. The Court can also order non-disclosure of

[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] Reply to the European Parliament questionnaire received from Cyprus.
[422] Reply to the European Parliament questionnaire received from Cyprus.
[423] Law 125(I) of 2018.
https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf.
[424] European Union Agency for Fundamental Rights, 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] European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update.

the information in light of the security interests of Cyprus[427].

264. Violating the protection of private communications is a de jure criminal offence. De facto, this illegality is often hidden behind the invocation of national security[428]. There is no legislation covering how the Police or other intelligence services use interception devices, who regulates interception procedures or how the protection of citizen's constitutional rights of citizens is guaranteed. The relevant regulations and protocols are currently pending discussion and approval in the House of Representatives. For the time being, this activity continues unchecked[429].

REDRESS

265. The legality of the actions of the Cyprus Intelligence service are evaluated by a three-member committee as provided for in Cyprus Intelligence Service Law 74(I)/2016. The Tripartite Committee is appointed by the Council of Ministers on the basis of a recommendation by the President of the Republic[430].

266. Law of 92(I)/1996 was amended in 2020 and strengthened the oversight framework of the Republic in particular the provisions on the Tripartite Committee. As part of its mandate, the Committee can initiate *ex officio* inquiries and start investigations into the facilities, technical equipment and archived material of the KYP. As stipulated by Article 17A(1) of Law 92(I)/1996 as amended by Law 13(I)/2020, the committee can also initiate inquiries into the Police' facilities, technical equipment and archived material. In light of these inquiries, the Committee can refer the matter to the Attorney General, the Commissioner for Personal Data Protection or the Commissioner of Electronic Communications and Postal Regulation for further action. The Committee also submits an annual report to the President of the Republic, in which it outlines its activities, formulates observations and recommendations and identifies omissions[431].

267. The President of Cyprus has a significant say in the composition of the Committee empowered to initiate critical inquiries in the actions of the KYP. In addition, the annual reports with the Committee's findings are first sent out to the President[432]. At the time of writing, there is no information on the exact composition of the Committee, its work or the scrutiny it performs[433].

KEY FIGURES IN THE SPYWARE INDUSTRY

268. Tal Dilian has played a key role in many of the developments in Cyprus and Greece. He

---

[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', Chapter 6, 2022.
[429] Philenews. 'Legal but uncontrolled interceptions'.
[430] Reply to the European Parliament questionnaire received from Cyprus.
[431] Reply to the European Parliament questionnaire received from Cyprus; CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020.
[432] Report by Fanis Makridis, PEGA Mission to Cyprus on 1 November 2022.
[433] Report by Fanis Makridis, PEGA Mission to Cyprus on 1 November 2022.

obtained Maltese citizenship in 2017[434]. Tal Dilian served in different leadership positions in the Israeli Defence Force for 25 years before he retired from the military in 2002[435]. He started a career as an 'intelligence expert, community builder and serial entrepreneur' in Cyprus, and then launched Aveledo Ltd., later to be known as Ws WiSpear Systems ltd. and after that Passitora Ltd[436].

269. In Cyprus, Dilian became closely associated with Abraham Sahak Avni. Avni has formerly been involved in the Israeli Police Special Forces as a special detective[437]. In November 2015, he acquired Cypriot citizenship and a golden passport through a EUR 2.9 million euro investment in real estate[438]. Avni founded the Cypriot NCIS Intelligence Services ltd[439], a company that was reportedly involved with the most powerful technology-oriented companies in the world[440]. NCIS Intelligence and Security Services provided security software to the Police Headquarters between 2014 and 2015 and provided training to employees of the Office of Crime Analysis and Statistics between 2015 and 2016[441]. The government Party, DISY, is also part of the company's clientele. Reportedly Avni installed security equipment in the party's offices[442]. In addition to Avni's security equipment, Dilian's materials were also sold to the Cyprus Drug Enforcement Agency and the Cypriot Police[443].

270. At one point, the Police Headquarters Crime Investigation Department identified violations of the confidentiality of private communications involving Avni's company. The police decided to close the case[444].

271. The connections between Dilian and Avni are numerous. Dilian's company WiSpear shared a building in Lacarna and some of its personnel with Avni[445]. In 2018, the two men launched Poltrex company, which was later renamed Alchemycorp Ltd. Poltrex has offices in the Novel Tower, as does Avni[446], and is also part of Intellexa Alliance. Reportedly, Avni's relations with the DISY party created the testing ground for Dilian's products[447].

DILIAN'S SPYWARE VAN

272. After the sale of Circles technologies and the founding of WiSpear, Tal Dilian also launched Intellexa Alliance in 2019, which according to its website is an'EU based and

---

[434] Government of Malta. Persons Naturalised Registered 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.

[438] Report by Fanis Makridis, PEGA Mission to Cyprus on 1 November 2022.

[439] Philenews, 'FILE: The state insulted Avni and Dilian'.

[440] Report by Fanis Makridis, PEGA Mission to Cyprus on 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] Report by Fanis Makridis, PEGA Mission to Cyprus on 1 November 2022.

[445] Report by Fanis Makridis, PEGA Mission to Cyprus on 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'.

regulated company with the purpose to develop and integrate technologies to empower intelligence agencies [448]. There are different surveillance vendors that fall under the marketing label of Intellexa Alliance, such as Cytrox, WiSpear (later renamed Passitora Ltd.), Nexa technologies and Poltrex Ltd. These different vendors in Dilian's group of companies allow Intellexa to supply and combine a broad assortment of surveillance software and services to its clients[449]. More detailed information on this corporate structure can be found in the chapter on the spyware industry.

273. On 5 August 2019, Dilian gave an interview to Forbes magazine about his black WiSpear van, showing off the different spyware capabilities that his alliance offers. This EUR 9 million worth van could hacking devices within a range of 500 meters[450]. The public attention generated by the Forbes interview[451] led to an investigation by the Cypriot authorities. Lawyer Elias Stefanou was appointed as independent criminal investigator for this investigation. During this inquiry, the authorities discovered another one of Dilian's undertakings that operated in Larnaca International Airport[452].

274. On 16 June 2019, Tal Dilian reportedly entered into a non-contractual arrangement with Hermes Airports to use his WiSpear equipment for the alleged purpose of enhancing the Wi-Fi signal for passengers at Larnaca International Airport, after which three Wi-Fi antennas were installed[453]. Although not registered in Cyprus, Israeli company Go Networks was also involved in the negotiations leading up to the arrangement[454]. The true reason for the agreement was however to test WiSpear's interception technology. The intercepted data of passengers was saved on the servers in the airport server room, close to the WiSpear office in Larnaca shared with Avni[455]. During the period when the antennas were operable, intercepted data was retrieved from 9 507 429 mobile devices[456].

275. Following the complaints against Dilian, Israeli Go Networks was reportedly associated with Intellexa by way of shared corporate ownership in Ireland. Former senior representatives of Israeli Go Networks were allegedly given top positions at Intellexa[457]. In addition, the police investigations found that export licences had been granted to WiSpear for 'interception equipment designed for the extraction of voice or data, transmitted over the air interface'[458] [459]. Dilian's companies, as stated by the Chamber of Commerce, have not received any export licences in the last two years. At the time of writing, it remains unclear who authorised these export licences[460].

---

[448] https://intellexa.com/.
[449] Haaretz, 'As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire'.
[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', Chapter 6, 2022.
[455] Makarios Drousiotis, 'Κράτος Μαφία', Chapter 6, 2022.
[456] Makarios Drousiotis, 'Κράτος Μαφία', Chapter 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. Chapter 6. Published 2022.
[459] Philenews. Export of tracking software from Cyprus.
[460] Inside Story, 'Who signs the exports of spyware from Greece and Cyprus?'.

276. The electronic data extracted from the confiscated equipment for the investigation was submitted for a three-level forensic examination by the police, an academic expert and Europol[461]. The van has remained in police custody, but it is not clear what has happened to the surveillance equipment. Allegedly, it has been returned to Dilian, but there seems to be no confirmation.

277. On 15 November 2021, a case was brought before the Criminal Courts with WS WiSpear Systems Ltd, Tal Dilian and two other WiSpear employees as defendants. Subsequently, Attorney General George Savvides upheld the case against the company WiSpear, but the criminal charges against Dilian and the employees were dropped[462]. The reasons for this decision are classified. However, the Attorney General could decide at any given moment to reopen the case against the three individuals.

278. WiSpear pleaded guilty to 42 charges and was fined EUR 76 000 in the Assize court on 22 February 2022[463]. WiSpear confessed to charges of illegal surveillance of private communications and data protection violations[464]. The Court published its final judgment, stating that: 'the Assize Court noted and qualified that the infringement attributed to the company never involved any intent, hacking [or] wiretapping, stating that there was never any attempt or purpose to personalize any data. The court emphasised that no damage was caused to any individual person'[465]. In addition to the fine imposed by the Assize court, Commissioner for Personal Data Protection Irini Loizidou Nicolaidou fined WiSpear EUR 925 000 for GDPR violations[466]. Although it was asserted that the black van episode touched on matters of national interest and critical infrastructure, the sanctions for the perpetrators were very light. This incident may have political significance beyond the violation of the privacy of passengers. Given that Cyprus is situated at a crossroads in many ways, there are several non-EU countries that could potentially have an interest in obtaining insight into traveller movements through Larnaca airport: Turkey, Israel, Russia and the US, for example.

279. Opposition party AKEL expressed outrage at the cases against Dilian and his staff being dropped and denounced the legal decision as a cover-up by the Attorney General[467]. After all, the Cypriot government had reportedly purchased equipment from Dilian's company and one of the accused employees had allegedly worked for NSO and provided training to the KYP on how to use the Pegasus spyware[468]. Dropping the charges ensured that the information on the links between Dilian's company and the Cypriot government would remain protected[469]. The Attorney General has refused to hand over the conclusions of the investigation, even though the PEGA Committee requested it during its official mission to Cyprus. This example shows that there are not

[461] Press Release of 10 August 2022 by the Deputy Attorney General acquired on the PEGA mission to Cyprus of 2 November 2022.
[462] Financial Mirror, 'Anger after 'spy van' charges dropped'.
[463] Makarios Drousiotis, 'Κράτος Μαφία', Chapter 6, 2022; Press Release of 10 August 2022 by the Deputy Attorney General acquired on the PEGA mission to Cyprus of 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.. Chapter 6. Published 2022.
[469] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.

full legal guarantees on data protection rights of individuals by mass surveillance equipment. While legal remedy exists on paper, judicial outcomes can be influenced by the government, leaving the individual victim defenceless. The investigation furthermore showed that Cyprus has become a ground for Cypriot-based companies to themselves experiment with surveillance equipment.

MOVE TO GREECE

280. Following the episode of the van and the lawsuit, Mr Dilian moved Intellexa's operations to Greece, although he never left Cyprus. He is reportedly planning his return to Tel Aviv[470]. Indirect links between several natural and legal persons registered in Cyprus and Greece expose the transfer of Dilian's businesses to Athens[471]. What follows are some of the names that are part of the Cyprus-Greece connections, although the main role of Intellexa SA in Greece is further explained in the chapter on Greece.

281. The judicial investigations led to the transfer of Mr Avni's and Mr Dilian's activities in Poltrex to Yaron Levgoren. Mr Levgoren is a permanent resident of Canada. He became the shareholder as well as director and secretary of Poltrex. Levgoren is also linked to Intellexa in Greece[472]. According to his Linkedin profile he currently represents the Greek-based Intellexa company Apollo Technologies.

SPYWARE COMPANIES AND CYPRUS

282. In addition to Intellexa Alliance, Cyprus was allegedly also home to NSO Group. In 2010 Tal Dilian, together with Boaz Goldman and Eric Banoun, launched the company Circles Technologies, specialised in the sale of systems that exploit SS7 vulnerabilities[473]. Six years later, Circles Technologies was sold to Francisco Partners for just under USD 130 million, of which USD 21.5 million went to Mr Dilian. This California-based private equity firm similarly obtained 90 % of NSO Group, resulting in the merger of Circles Technologies and NSO Group under L.E.G.D Company Ltd., known as Q Cyber Technologies Ltd., since 29 March 2016[474].

283. According to the response from the Cypriot Government to the PEGA Committee, the Department of Registrar of Companies and Intellectual Property does not include a registered legal entity of NSO Group. NSO Group does not hold shares in any legal entity registered in Cyprus. However, individual board members of NSO Group have either established or bought six companies. In addition, the Pegasus spyware does not appear to have been developed in or officially exported from Cyprus[475].

284. Expansion under Francisco Partners between 2014 and 2019 did include six Cypriot companies. Francisco Partners was supplemented with ITOA Holdings Ltd., registered in Cyprus and parent company of CS-Circles Solutions Ltd., Global Hubcom Ltd. and MS Magnet Solutions. Ms Magnet Solutions owns Mi Compass Ltd. CS-Circles

[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.
[474] Amnesty International, Operating from the Shadows.
[475] Reply to European Parliament questionnaire received from Cyprus.

Solutions Ltd., furthermore, owns CI-Compass Ltd. In addition to the Cypriot entities, CS-Circles Solutions Ltd. also owns Bulgarian entities. NSO Group has stated that 'the Bulgarian companies provide, on a contract basis, research and development services to their respective Cypriot affiliates and export the network products for governmental use.'[476].

285. The Cypriot Government denies the export and development of Pegasus. However, on 21 June 2022, NSO official Chaim Gelfad did state that NSO companies in Cyprus and Bulgaria were engaged in software providing intelligence services[477]. According to a document shared by opposition party AKEL to the European Parliament, NSO Group has reportedly exported the Pegasus spyware through one of its subsidiaries in Cyprus to a company in the United Arab Emirates. One of the subsidiaries reportedly issued an invoice of USD 7 million for services to the company in question[478]. This information cannot, however, be confirmed.

286. Reportedly, NSO Group also had an active company in Cyprus that allegedly hosted a customer service centre. In 2017, a meeting with NSO officials and Saudi Arabian customers took place in the Four Seasons Hotel in Limassol to present to them the latest capabilities of the Pegasus 3 version spyware. This version had the novel zero-click capability that could infect a device without the necessity of clicking on a link, for example through a missed WhatsApp call. The Saudi Arabian clients immediately purchased the technology for USD 55 million[479] [480]. It should be noted that a year later, on 2 October 2018, the Saudi regime killed Jamal Khashoggi in the Saudi consulate in Turkey, after surveilling his near ones with Pegasus. This is disputed by NSO.

287. According to CitizenLab, 25 state actors were clients of Circles Technologies in 2020. Amongst these state actors were Belgium, Denmark, Estonia and Serbia[481]. In 2020, NSO Group closed its Circles office in Cyprus. At the time of writing, it remains unclear which Circles companies remain in operation[482].

288. The Israeli QuaDream is another company that is reportedly linked to the export of its spyware product 'Reign' from Cyprus. In April 2023, media reported that QuaDream was shutting down its Israeli offices[483]. Through InReach, a company registered in Cyprus since 2017, QuaDream products were indirectly sold to customers and thus circumvented Israeli export controls. The two companies are in an ongoing legal dispute[484].

289. The current director and secretary of InReach is A.I.L. Nominee Services Ltd. This company was already registered in Cyprus in 2010 and its founding shareholder was the

[476] Amnesty International, Operating from the Shadows.
[477] Report by Fanis Makridis, PEGA Mission to Cyprus on 1 November 2022.
[478] Akel report, PEGA mission to Cyprus.
[479] Makarios Drousiotis, Κράτος Μαφία, Chapter 6, published in 2022.
[480] Haaretz, Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals.
[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.

current Deputy Attorney-General Savvas Angelides[485]. Mr Angelides sold his shares in A.I.L. Nominee Services to Christos Ioannides on 16 February 2018, a few weeks before he became Minister of Defence[486]. However, A.I.L. Nominee Services remains the director and secretary of InReach[487] and thus in business with a company exporting QuaDream products to third countries.

290. In 2011, Abraham Sahak Avni founded a company with Michael Angelides, the brother of the former minister and current Deputy Attorney-General Savvas Angelides. Their company S9S was registered with the Registrar of Companies on 10 November 2011[488] with the assistance of the former law firm of Savvas Angelides[489]. In addition, A.I.L. Nominee Services ltd was identified as the secretary of S9S. During that time, Savvas Angelides was still the main shareholder in A.I.L. Nominee Services[490]. The partnership between Michael Angelides and Mr Avni was, however, dissolved in 2012. Savvas Angelides became Deputy Attorney-General in 2020 and was the person in charge of investigating Mr Avni and Mr Dilian in the case of the surveillance van[491]. In a press statement on 10 August 2022, the Deputy Attorney-General declared that neither he nor his relatives had any connection with Tal Dilian. On the partnership between Michael Angelides and Mr Avni, he mentioned that the 'professional cooperation failed from the outset, coupled with the fact that the company registered by my former law firm, on the instructions of my relative, was never activated' and therefore never formed an 'impediment to my involvement in the decision regarding the "Black Van' case"'[492] . However, the press statement does not make any reference to Savvas Angelides' company A.I.L Nominee Services ltd. that was activated in July 2010[493], nor to the role of the company as secretary in the partnership between his relative and Mr Avni in S9S.

*BLACK CUBE*

291. Black Cube is a company employing former officers of Israeli Intelligence Agencies, such as Mossad. The company uses operatives with fake identities. According to the *New Yorker*, former CEO of NSO Group Shalev Hulio hired Black Cube after three lawyers – Mazen Masri, Alaa Mahajna and Christiana Markou – sued NSO and an affiliated subsidiary in Israel and Cyprus[494]. In 2018, the three lawyers received several messages from so-called acquaintances of certain firms and individuals, proposing meetings in London. Hulio stated that 'For the lawsuit in Cyprus, there was one

[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] Press Release, Deputy Attorney General of 10 August 2022 as acquired during the PEGA mission to Cyprus on 2 November 2022.
[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.
[491] Report by Fanis Makridis, PEGA Mission to Cyprus on 1 November 2022.
[492] Press Release, Deputy Attorney General of 10 August 2022 as acquired during the PEGA mission to Cyprus on 2 November 2022.
[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.

involvement of Black Cube' since the lawsuit 'came from nowhere and I want to understand'[495]. Black Cube was also exposed in spying scandals in Hungary and Romania.

PURCHASE AND USE OF SPYWARE BY CYPRUS

292. Besides the facilitation of a welcoming export climate for spyware companies, the Cypriot Government itself has a history of purchasing spyware. It has also allegedly used surveillance systems itself. At the time of writing, it remains unclear in which cases Cyprus made use of conventional surveillance methods or spyware.

293. After the elections of 2013, Andreas Pentaras was appointed as head of the Cyprus Intelligence Service, while surveillance expert Andreas Mikellis was responsible for the protection of President Anastasiades' communications. In that same year, Mr Mikellis reportedly visited the ISS surveillance exhibition in Prague, where he allegedly negotiated with Hacking Team for the purchase of the so-called DaVinci software[496]. The DaVinci software was able to infect applications of a mobile telephone and therefore did not meet the official requirements for the lifting of privacy[497].

294. Disclosed contact information as revealed by WikiLeaks between Mr Mikellis and Hacking Team indicated the bypassing of tender procedures and failure to properly review the acquired surveillance system. At the start of 2014, the software was reportedly installed and four employees of the KYP were trained, including Mr Mikellis[498].

295. When WikiLeaks revealed the purchase of Hacking Team's surveillance software, the KYP confirmed that this system was used for national purposes only[499]. Despite Mr Mikellis' contact with Hacking Team[500], it was the head of the KYP Andreas Pentaras who ultimately resigned after these revelations came to light[501]. Kyriakos Kouros replaced Mr Pentaras.

296. According to WikiLeaks, one other police department was reportedly also interested in purchasing a communications surveillance system from Hacking Team. This department tried to secure this system through Sahak Avni[5021a]. It is, however, unclear which police department is at issue here**.**

TARGET MAKARIOS DROUSIOTIS

297. Starting in February 2018, investigate journalist Makarios Drousiotis was allegedly spied on by the Cypriot Government using both eavesdropping techniques and

[495] The New Yorker*,* How Democracies Spy on their Citizens.
[496] Makarios Drousiotis, Κράτος Μαφία, Chapter 6, published in 2022.
[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.

spyware[503]. This case of espionage started during the time when Mr Drousiotis was assistant to the Cypriot EU Commissioner for Humanitarian Aid and Crisis Management Christos Stylianides and during his inquiries into the financial connections between President Anastasiades and Russian figures such as oligarch Dmitri Rybolovlev. According to Mr Drousiotis, it was his latter role that triggered the first surveillance attempt[504].

298. In the course of Mr Drousiotis' inquiries into the Russian connections, revelations about NSO Group operating from Cyprus started to appear in international media outlets, including on the Pegasus 3 presentation in the Four Season Hotels. CitizenLab, moreover, suspected Cyprus to be one of the countries using the NSO technologies for intercepting communications of the British Foreign Office computer systems[505]. At this point, Mr Drousiotis started to recall several indications of the Pegasus spyware infiltrating his telephone, including a missed WhatsApp call, rapid battery depletion and the frequent overheating of his device without him using it[506]. In the light of these events, Mr Drousiotis believes that the Cypriot Government – in particular the Cyprus Intelligence Service – was behind the infection of his telephone.

299. In May 2019, Mr Drousiotis sent a letter to President Anastasiades expressing his concerns about the surveillance of his telephone, outlining the potential motives behind this surveillance, as well as holding the President personally accountable for whatever may happen to him after the espionage. Mr Anastasiades forwarded the letter to the current head of the Cyprus Intelligence Service, Kyriakos Kouros. Both Mr Anastasiades and Mr Kouros have refuted the alleged surveillance with the Pegasus software, reiterating that NSO Group was in fact not even registered in Cyprus[507].

300. In the months that followed, several intimidation attempts occurred including the disappearance of evidence on his computer, the disconnection of security cameras at Mr Drousiotis' home and being tracked by strangers. After going public with his story and filing a complaint with the Cypriot police, Mr Drousiotis contacted Lambros Katsonis, Head of the Technical Support Department of Panda Security, a Cypriot company specialised in antivirus equipment. Mr Drousiotis was, however, unware of the fact that the Cypriot Government also used this antivirus software for its own devices. Against this background, Katsonis seems to have been sent to Mr Drousiotis' home under false pretences, possibly with the aim of further infiltrating Mr Drousiotis' devices as instructed by the KYP[508].

301. In 2019, Mr Drousiotis became aware of suspicious entries on his Android telephone and contacted Google One Support to confirm the nature of these entries. However, Google does not in general respond to surveillance-related matters and referred the customer in question to the national law-enforcement agencies1a.Although Mr Drousiotis did not have any confidence in the police, he did agree to hand over his

[503] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/
184 Makarios Drousiotis, Κράτος Μαφία, Chapter 5, published in 2022.
[504] Makarios Drousiotis, Κράτος Μαφία, Chapter 5, published in 2022.
[505] BBC, No 10 network targeted with spyware, says group.
[506] Makarios Drousiotis, Κράτος Μαφία, Chapter 5, published in 2022.
[507] Makarios Drousiotis, Κράτος Μαφία, Chapter 5, published in 2022.
[508] Makarios Drousiotis. Κράτος Μαφία. Chapter 5. Published in 2022.

devices for forensic examination[509].

CONCLUDING REMARKS

302. Cyprus has a robust legal framework for the protection of personal data and privacy, for the authorisation of surveillance and for exports. However, in practice it would seem that rules are easy to circumvent and there are close ties between politicians, the security agencies and the surveillance industry. It seems to be the lax application of the rules that makes Cyprus such an attractive place for trade in spyware. Better implementation of existing rules is needed. Cyprus is also of considerable strategic interest to Russia, Turkey and the US. Furthermore, close relations with Israel seem to be of particular mutual benefit with regard to trade in spyware. Export licenses for spyware have become a currency in diplomatic relations.

*I.E. Spain*

303. Following the invitation by the PEGA Committee, the Spanish Authorities were invited to a hearing on 29 November 2022 to give account of the use of spyware surveillance in Spain, to the extent possible within their legal obligations. Due to these stated 'legal constraints', the answers given to the Committee were limited and left most questions open.

304. The PEGA Committee visited Madrid in March 2023. The delegation met with the State Secretary for European Affairs and people who according to CitizenLab were targeted with spyware, namely the President of the regional Government of Catalonia, the Catalan regional Minister of Foreign Action, and a Councillor at Barcelona City Council. They also met members of the Catalan Parliament's Inquiry Committee on Pegasus, a representative of the Ombudsman's office, NGOs working in the area of fundamental rights and journalists.

305. The July 2021 revelations by the Pegasus project showed a large number of alleged targets in Spain. However, they seem to have been targeted by different actors and for different reasons. In May 2022, a report in *The Guardian* newspaper identified Morocco as possibly having spied on more than 200 Spanish mobile phones. The Spanish government confirmed that Prime Minister Pedro Sánchez, Minister of Defence Margarita Robles and Minister of the Interior Fernando Grande-Marlaska had been infected by Pegasus spyware, while Minister of Agriculture Luis Planas was targeted but not infected[510]. It is also suggested that the mobile phone of erstwhile Foreign Minister Arancha González Laya was also spied on, although it has not been possible to establish the origin of the cyberattack or whether it was compromised using Pegasus. The targeting of a second group of targets is referred to as 'CatalanGate'[511]. It includes Catalan parliamentarians, Members of the European Parliament, lawyers, journalists, civil society organisation members, academics and some family and staff connected to

[509] Makarios Drousiotis. Κράτος Μαφία. Chapter 5. Published in 2022.
[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 May 2022.
[511] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022.

those targets[512], which can be referred to as 'indirect' or 'relational' targeting. The CatalanGate surveillance scandal was first reported on in 2020, after a joint investigation by *The Guardian* and *El País*[513], but it was not until April 2022 that CitizenLab completed their in-depth investigation and the scale of the scandal was revealed. The results of that probe showed that at least 65 persons were targeted[514]. It should be noted that as of December 2022 CitizenLab acknowledged that one infection was incorrectly attributed due to an error in labelling of initials[515], although the overall number of Catalan targets remained unchanged. In May 2022, the Spanish authorities admitted to targeting 18 individuals with court authorisation[516], although the warrants for those cases have not been made public. The former director of the Spanish National Intelligence Centre (CNI) Paz Esteban appeared before the Official Secrets Committee of the Parliament at a meeting held in camera to provide justification for the surveillance of these 18 persons.

306. The Spanish government has given limited information so far on their role in this targeting, invoking the need for confidentiality for national security and legal reasons. However, on the basis of a series of indicators[517], some of which were acknowledged at the aforementioned Official Secrets Committee, it is assumed that the surveillance of the Catalan targets was conducted by the Spanish authorities.

307. A close analysis of the surveillance shows a clear pattern. Most of the CatalanGate interceptions coincide with and relate to key political events, issues or figures, such as the admissibility of the disconnection laws by the Catalan Parliament, the court cases against Catalan separatists, public rallies organised by Tsunami Democràtic and communications with Catalan separatists living outside Spain[518]. Such surveillance includes for example the lawyer-client communications of a jailed separatist on the eve of his trial, contacts between spouses or communications relating to the taking up of seats in the European Parliament. With regard to the remaining 47 spyware cases, it has not been possible to assess how the targets would have had an immediate impact on national security or the integrity of the state or how they constituted an imminent threat to these, and no information was provided on this[519]. Although some targeted persons had faced criminal charges before they were targeted, no criminal charges have been brought against any of the 18 persons targeted as a result of spyware surveillance[520].

---

[512] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022* at pg. 1.
[513] https://www.theguardian.com/world/2020/jul/16/two-catalan-politicians-to-take-legal-action-targeting-spyware
**[514]** Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022* at pg. 1.
[515] Citizen Lab*, Correcting a case,* CatalanGate report https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/ 22 December 2022.
[516] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , 5 May 2022.
[517] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at pg. 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.
[520] Mission to Spain.

PURCHASE OF SPYWARE

308. The Spanish authorities have previously acknowledged the purchase of tools for the interception of telecommunications and the acquisition of SITEL (Systems for the Lawful Interception of Telecommunications) in 2001. They also acknowledged that spyware services were contracted from Hacking Team in 2010 by the Ministry of the Interior, CNI and the Spanish National police as part of the implementation of the Integrated Telecommunications Interception System, which provided the operational units of the State Security and Corps (FCSE) with the means for the interception and recording of electronic communications authorised by a court order[521]. Since its acquisition, SITEL has been used by the Spanish authorities, among others, in anti-drug operations, to locate the members of the jihadist cell behind the attacks in Madrid on 11 March 2004 and to fight cases of political corruption. It was also previously reported by CitizenLab that Spain was a suspected customer of Finfisher[522]. In 2020, the Spanish newspaper *El Pais* reported that Spain has done business with NSO Group and that the CNI routinely uses Pegasus[523]. The Spanish government allegedly purchased the spyware in the first half of the 2010s for an estimated EUR 6 million[524] [525]. The purchase of SITEL was confirmed by former Vice-President de la Vega in 2009[526], while the contracting of Hacking Team's services was acknowledged by the CNI in a comment made to the newspaper *El Confidencial* in 2015[527]. In addition, a former employee of NSO has further confirmed that Spain has an account with the company[528] although the Spanish authorities declining to comment or confirm[529].

309. According to Google's Threat Analysis Group (TAG), spyware company Variston IT is based in Barcelona and is allegedly linked to a framework that exploits n-day vulnerabilities in Microsoft Defender, Chrome and Firefox, installing spyware on targeted devices. These vulnerabilities were fixed in 2021 and early 2022[530]. According to its website, Variston offers 'tailor-made Information Security Solutions'[531].

LEGAL FRAMEWORK

---

[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 at pg. 5.
[523] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at pg. 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 May 2022.
[527] El Confidencial, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/ 6 July 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.
[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/.*

310. The right to privacy is protected under Article 18 of the Spanish Constitution of 1978, including the right to secrecy of communication, and in particular guarantees 'postal, telegraphic and telephone communications[532]'. The use of spyware such as Pegasus and Candiru would be a violation of Article 18 without a court order, but this possibility is provided for under Spanish law[533]. The constitution also provides for further exceptions to those rights in Part I Section 55 by stating that some rights can be suspended subject to the 'participation of the courts and proper parliamentary control' if it has been agreed to declare a state of emergency or siege under the terms provided for in the Constitution or in the case of individuals under investigation for activities relating to armed groups or terrorist organisations[534]. Furthermore, Article 55 includes democratic safeguards to ensure that 'unjustified use or misuse' of those powers will give rise to criminal liability.

311. For activities that may affect the inviolability of the home and the secrecy of communications, Article 18 of the Spanish constitution requires a court order. Article 8 of the ECHR requires that any interference with the exercise of this right by a public authority must be in accordance with the law and constitutes a measure that in a democratic society is necessary for national security, public safety, the economic interest of the country, the protection of public order and the prevention of crime, the protection of health or morality and the protection of the rights and freedoms of others.

312. Further details on the exemptions to the right to privacy in Article 18 are provided for in the Criminal Procedure Act[535] [536]. Article 588 of this Act specifically limits the use of investigative measures to the investigation of facts which, due to their particular seriousness, justify the limitation of fundamental rights. Nevertheless, the cases provided for in the following are excluded from this provision: a) Organic Law 2/2002, of 6 May regulating the prior judicial control of the National Intelligence Centre; b) Organic Law 4/1981 of 1 June on states of emergency, exception and siege; and c) Organic Law 2/1989 of 13 April on Military Procedure, which contains supplementary provisions applicable to the Law on Criminal Procedure. Article 588 of the Act requires authorisation to be provided by a judge for the interception of telephone and telematic communications when the investigation is into serious crimes such as terrorism or crimes committed through computerised instruments or any other information or communication technology or communication service. In addition, limitations must be authorised by a judicial authority. Authorisations are subject to four specific principles: firstly, specialisation (that the surveillance is related to a specific crime); secondly, adequacy (outlining duration, objective and the subjective scope); thirdly, proportionality (strength of available evidence, severity of the case and result sought),

---

[532] Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx , at Section 18.

[533] Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx**,** Section 18.

[534] Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx , at Section 55.

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

[536] Royal Decree of 14 September 1882 approving the Criminal Procedure Act, https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20220907.

and finally exceptional nature and necessity (there are no other measures available and without it, the investigation will be interfered with)[537]. Article 588 *septies* (a,b and c) specifically stipulates the conditions for remote computer searches. The competent judge may authorise under Article 588 *septies* the installation of software, allowing remote and telematic examination without the knowledge of the owner or user, provided that it relates to the investigation of certain criminal offences. To that end, the measure is strictly limited to a strict duration of one month, extendable for periods of one month up to a maximum of three months.

313. Article 197 of the Criminal Code provides for penalties ranging from 12 months to four years imprisonment and a fine of 12 to 24 months for persons who seize or intercept inter alia electronic mail and telecommunications without correct permission[538]. Additionally, Article 264 of the Code of Criminal Procedure further regulates the criminal act of erasing or deleting data and allows access to the data in situations where the required authorisation has been granted by a competent authority[539].

314. The requirements for judicial supervision are: a) the Judicial Police must inform the examining magistrate about the implementation and results of the measure; b) in the enabling judicial decision, the judge specifies the frequency and form in which the judicial police must inform them about the implementation of the measure; c) within the established deadlines, the Judicial Police must make available to the judge two different digital files, one with the transcription of the passages considered to be of interest and the other with the complete recordings; d) the recordings must indicate the origin and destination of each of the communications; e) the Judicial Police must use an advanced electronic sealing or signature system or a sufficiently reliable warning system to guarantee the authenticity and integrity of the information transferred from the central computer to the digital media on which the communications have been recorded, and; f) the judicial police must report back with the results of the measure when the implementation of the measure is concluded.

315. The Spanish intelligence service is made up of three main agencies. Firstly, the National Intelligence Service (CNI) which achieves its missions by collecting information in Spain and overseas and acts under the supervision and control of the executive, legislative and judicial powers and is attached to the Ministry of Defence[540]. The Director of the CNI is nominated by the Minister for Defence and serves as the Prime Minister's lead advisor on issues relating to intelligence and counter-intelligence[541]. The second body is the domestic intelligence agency, the Intelligence Centre for Counter-Terrorism and Organised Crime (CITCO). The third body is the Spanish Armed Forces Intelligence Centre (CIFAS). The CIFAS is also under the direct supervision of the

---

[537] . Criminal Procedure Act 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf .
[538] Criminal Code 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf , at Article 197.
[539] Criminal Procedure Act, 2016 https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf at Article 264.
[540] National Intelligence Centre (CNI), https://www.cni.es/.
[541] https://www.cni.es/en/intelligence.

Ministry of Defence[542] [543]. The CNI was established under Law No 11/2002 of 6 May 2002, pursuant to which it is authorised to conduct 'security investigations'[544]. The country's police and law enforcement agency, the Guardia Civil, is of a "military nature" and also accountable to the Ministry of Defence[545].

316. The Official Secrets Law, which dates back to 1968, covers classified documents in Spain and does not outline a declassification time period after which an official secret expires[546]. Unless the government specifically orders the release of documents, i.e. the express declassification of a document by a ministry or other official body, such documents remain secret. This law is currently under review by the Spanish government, and though no deadline has been set for its adoption, a preliminary draft law on classified information was approved on 1 August 2022. It provides that classified information will have to be published within a period of between 4 and 50 years, although this may be extended.

*EX ANTE* SCRUTINY

317. The mission of the CNI is to provide the Spanish government with the information and intelligence necessary to prevent and avoid any risk or threat that affects the independence and integrity of the state, national interests and the stability of the rule of law and its institutions. Much of the surveillance conducted in Spain was carried out by the CNI. The CNI was established under Law 11/2002 of May 6, which grants the CNI powers to conduct 'security investigations'on persons or entities'[547]. However, there is little clarity on the means used for or limitations to such activities[548], as the CNI's activities, its organisation and internal structure, means and procedures, personnel, facilities, data bases and data centres, sources of information and information or data that may lead to knowledge of the above matters are classified information with the relevant degree of secrecy[549]. Law 11/2002 also established parliamentary, executive and legislative oversight over the CNI[550]. Parliamentary oversight is carried out by the Committee on the use and control of credits allocated to secret funds (the Official Secrets Committee) of the Spanish Parliament, which was established in 1995[551]. Because of the delayed constitution of the committee during the 14th term of the Spanish Parliament (elected in December 2019), the Official Secrets Committee has not submit its annuals report on the activities of the CNI, as required by law. By April 2023,

[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 at pg. 40.
[544] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html Article 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.
[547] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html at Article 5.5.
[548] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain , 4 May 2022.
[549] Law 11/2002, of May 6, Regulating the National Intelligence Centre, at Article 5.1.
[550] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html at Article 11.
[551] Law 11/1995 May 11, https://www.boe.es/eli/es/l/1995/05/11/11/con .

no annual report has been submitted during this parliamentary term. The Government Delegated Committee for Intelligence Affairs co-ordinates the intelligence activities of all Spanish intelligence and information services[552]. Lastly, the Defence Committee of the Congress of Deputies conducts legislative oversight over the CNI[553]. The annual Intelligence Directive sets the intelligence priorities of the CNI .

318. Judicial control over the actions of the CNI is provided for in Organic Law 2/2002 May 6[554] [555], which complement Law 11/2002 of 7 May regulating the CNI. In particular, this regulation requires that when the CNI seeks to conduct surveillance, the CNI Secretary of State Director has the obligation to request authorisation from a competent magistrate of the Supreme Court in accordance with the Organic Law of the Judiciary, to authorise the adoption of measures affecting the inviolability of the home and the secrecy of communications[556], provided that such actions are necessary for the CNI to perform the its functions. In addition, the Law stipulates that surveillance operations cannot last more than three months and that any extension of this period must be properly justified. However, these provisions were brought into force at a time when surveillance technology was far less advanced and spyware such as Pegasus and Candiru did not exist. The legal safeguards risk therefore being outdated and do not provide citizens with sufficient protection. Therefore the Executive announced that it would reform the legal framework of the CNI, but no proposals have been submitted yet.

*EX POST* SCRUTINY

319. The laws establishing the CNI also established the Defence Committee of the Congress of Deputies which is responsible for allocating the secret funds for the CNI and for drafting an annual report on the CNI.The amounts assigned to secret funds are set in the Spanish general budget law for each financial year[557]. All the bodies that are tasked with oversight of the CNI, such as the Defence Committee, the Official Secrets Committee or the Ombudsman, have access to the information needed to assess whether operations were pursued lawfully and correctly. The Government annually determines and approves the objectives of the CNI through the Intelligence Directive, which are secret[558] [559]. The Director of the CNI has exclusive competence to decide on the purpose and destination of the funds assigned, and periodically has to report on their use to the Prime Minister. The Official Secrets Committee is informed about the intelligence objectives and has the prerogative to submit an annual report on the activities of the

[552] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html at Article 6.
[553] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html at Article 11.
[554] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain , 4 May 2022.
[555] Organic Law 2/2002 May 6, 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.
[556] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain , 4 May 2022.
[557] Law 11/1995, of May 11, regulating the use and control of credits allocated to secret funds, Article 2, https://www.boe.es/eli/es/l/1995/05/11/11/con.
[558] Law 11/2002, of May 6, regulating the Intelligence Nacional Centre (CNI), at Article 3.
[559] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022, p. 2.

intelligence services[560]. It also has access to the Director of the CNI's annual report on the assessment of the CNI's activities, situation and the extent to which it has met its objectives. However, Spanish law does not stipulate that public access will be granted to documents or information relating to the work of the intelligence services. This requirement is also notably absent in the legal framework of the Law on Transparency[561]. Given this secrecy, it cannot with any certainty be determined whether the Spanish government concluded contracts with NSO Group or whether it acquired and used Pegasus. The persons targeted do not know the reasons, scope and consequences of the interception of their communications[562].

320. As result of the revelation that the CNI has used Pegasus and Candiru, the Spanish Ombudsman announced an *ex officio* investigation[563]. The Spanish Ombudsman's official statement of 18 May 2022 acknowledged that the Council of Ministers had granted the Ombudsman full access to classified documents to the Ombudsman, not making use of its prerogative provided for in Article 22 of Organic Law 3/1981 on the Ombudsman. However, this investigation only concerned the 18 persons that the Spanish authorities have confirmed had been targeted with court authorisation[564] [565]. The investigation concluded that the interceptions had been carried out within the law because it established that they had been approved by a court and the authorisation was accompanied by the required justification[566]. However, the Ombudsman does not have the competence to assess proportionality, which can only be determined by a judge[567]. He also did not contact or interview any of the targeted persons or their lawyers. The Ombudsman recommended a review of current legal provisions and reforms where necessary to reflect the modernisation of surveillance systems[568]. Following this, the Spanish government announced in May 2022 that there would be a review of the Official Secrets Act of 1968 and the Organic Law 2/2002[569] [570], but no timeframe has been set for adoption of this review.

321. The Official Secrets Committee is required to submit an annual report on the activities of the intelligence services. It was convened on 5 May 2022 in the light of the surveillance activities of the CNI, but this was the first meeting of the body in more than

---

[560] Law 11/1995, of May 11, regulating the use and control of credits allocated to secret funds, at Article 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 at p. 2.
[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 May 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 May 2022.

[567] Information from 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 May 2022.
[570] https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx , 26 May 2022.

three years becaise of the disruption of parliamentary activity caused by the COVID-19 pandemic. Head of the CNI Paz Esteban appeared before the Committee and admitted to the surveillance of 18 leaders of the separatist movement. She also submitted the court orders for those 18 cases to the Committe[571] [572]. However, in accordance with Article 5.5 of Law 11/2002, the hearing was conducted in camera and those present were not allowed to enter with any electronic devices[573].No official information was made available except for the number of cases. According to the spokespersons present at the hearing, it was almost exclusively focused on the Catalan targets, and not on Pedro Sánchez, Margarita Robles and the alleged 3GB of data that was taken from their devices using mercenary spyware[574]. Robles has repeatedly insisted that the targeting of the 18 Catalan targets was justified.

322. Sánchez has also spoken on the issue in the Spanish Parliament, where he once again reiterated that everything has been done within the law and that national security is subject to the oversight of the Spanish Parliament and other government bodies[575]. Former NSO Group CEO Shalev Hulio also claimed that the use of Pegasus was entirely legal when told the *New Yorker* that the use of Pegasus by Spain was legitimate given Spain's strong respect for the rule of law and the requirement for Supreme Court authorisation[576].

323. On 3 May 2022, the Spanish Congress voted against a proposal to establish a committee of inquiry on the use of Pegasus. On 21 September 2022, the Catalan parliament established a committee of inquiry on espionage of political representatives, activists, journalists and their families by the Kingdom of Spain with the Pegasus and Candiru programmes.

PUBLIC SCRUTINY

324. Since revelations came to light in April 2022, there has been a significant amount of public scrutiny on the use of spyware against members of the Spanish government and Catalan independence advocates. The Spanish media and media outlets around the world have worked intensively with civil society organisations to scrutinise the surveillance system in Spain and advocate for the fundamental rights of the persons targeted. Conversely, some Spanish politicians have tried to discredit CitizensLab, suggesting their methods are unsound or that they are politically motivated.

REDRESS

---

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

325. A legal case on the spyware surveillance of Prime Minister Pedro Sánchez and Minister for Defence Margarita Robles was filed by the Solicitor General[577] at the Spanish National Court (SNC), the Audiencia Nacional in Madrid. The jurisdiction of the SNC is provided for in Article 65.1a of the Organic Law 6/1985 on the Judiciary, and under this the alleged facts fall within the SNC's jurisdiction as they affect persons in high-ranking national bodies, such as the Prime Minister and the Minister of Defence. Judge José Luis Calama, head of the Central Court of Instruction number 4, is responsible for this on-going case[578]. On 13 October 2022, Judge Calama submitted a questionnaire to Robles and Grande-Marlaska, which included a request, to be confirmed by legal sources, about how the Pegasus infections were identified. The Prosecutor's Office and the Office of the State Attorney also sent questions to the Ministers[579].

326. Legal complaints on spyware surveillance have been filed in Investigative Court in Barcelona by individuals with direct or indirect ties to the Catalan independence movement, with investigations are ongoing, albeit at a slow pace. The first complaint was filed in 2020 by Roger Torrent, former President of the Catalan Parliament and current Minister of Business and Work of Catalonia, and Ernest Maragall, former Minister of Foreign Action, Institutional Relations and Transparency of Catalonia and current ERC President of Barcelona City Council, [580] [581]. The case was allocated to Investigative Court number 32 in Barcelona, which provisionally closed the case. Andreu Van Den Eynde is one of the lawyers representing Torrent and Maragall in this case, and has been targeted with Pegasus himself. Van Den Eynde has criticised the courts consistently delaying proceedings and virtually 'paralysing' the case[582]. Omnium Cultural, the Catalan National Assembly (ANC) and the Popular Unity Candidacy party (CUP) have also filed several criminal complaints in the same court in Barcelona, but no investigation has yet been opened. Investigative Court number 32 in Barcelona rejected to the request to joint lawsuits so they are now being dealt with by different courts and judges. The complaints of Òmnium Cultural and CUP were allocated to Investigative Court number 21 in April 2022, and those of ANC to Court 23 on July 26th 2022. The complaints have not yet been fully allowed to proceed, nor has it been agreed to initiate investigations, so none of these cases is being investigated. Most of the cases have been shelved by the judges until more evidence is gathered, since the key evidence - the allegedly infected mobile phones - were no in the plaintiffs' possession [583]. Judges may decide to accept the reports by CitizenLab as expert evidence in the case. However, if the judges do not allow this, it makes it difficult for the targeted

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

persons to prove their case[584].

327. As the SNC has jurisdiction in the whole of Spain over the most serious crime cases, the public prosecutor could request that all Pegasus cases to be joined[585]. In other words, the cases of those targeted by the Spanish government and the CatalanGate targets would all be heard in the SNC in Madrid. The lawyers representing the Catalan targets assert that there is no link between the cases unless the perpetrator is proved to be the same in all instances of surveillance[586].

328. There are a number of other pending legal cases linked to the 65 Catalan targets. One such case was filed by lawyer and Pegasus target Gonzalo Boye on behalf of at least 19 targets against NSO, its three founders Niv Karmi, Shalev Hulio and Omri Lavie, Q Cyber Technologies, and OSY, a subsidiary company based in Luxembourg[587] [588]. Former President of Catalonia Quim Torra and former Vice-President of the Catalan Parliament Josep Costa have filed a complaint at the Supreme Court, but one year on it has yet to be decided by the judiciary whether the case should be tried before the Supreme Court or the SNC. No investigation has taken place in the meantime. There also is legal action under way in France, Belgium, Switzerland, Germany, and Luxembourg on the surveillance of Catalan separatists in exile [589].

THE TARGETS

329. The targeting with spyware of members of the Catalan pro-independence movement and family and staff linked to them allegedly began as early as 2015, when the then president of the Catalan National Assembly (ANC), Jordi Sánchez, was targeted shortly after a large demonstration in Barcelona. According to the April 2022 Citizen Lab report, at least 65 persons were targeted with spyware between 2017 and 2020: 63 with Pegasus, four with Candiru and at least two people with both[590]. At least 51 individuals' devices were successfully infected[591]. Among those allegedly targeted, directly or indirectly, were pro-Catalan independence political figures, such as Minister of Business and Employment and former President of the Catalan Parliament, Roger Torrent; current Esquerra Republicana de Catalunya (ERC) President in Barcelona City Council and former Minister of Foreign Action, Institutional Relations and Transparency of Catalonia, Ernest Maragall; and four members of the European Parliament. Given the significant passage of time since the beginning of the hacking and these revelations, a number of targets were unable to be identified or further

[584] Mission to Spain.
[585] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , 2 May 2022.
[586] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , 2 May 2022.
[587] El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html , 3 May 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.
[590] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at p. 5.
[591] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at p. 5.

investigated owing to various factors, including a number of targets who disposed of the phone in question[592].

330. Spanish Prime Minister Pedro Sánchez, Minister for Defence Margarita Robles and Minister of the Interior Fernando Grande-Marlaska were targeted with Pegasus between May and June 2021[593]. There is little information available so far on the details of this hacking, as they were announced by the government and were not the result of an investigation by Citizen Lab or any other such research service or by investigative journalists, and are still part of an ongoing investigation. Sánchez and Robles are the heads of the two government branches that oversee the CNI, the body responsible for conducting surveillance in Spain. The infected devices of Sánchez and Robles were government-issued and were being scanned for spyware occasionally[594]. Grande-Marlaska was infected on his personal device[595]. Minister for Agriculture Luis Planas, who had formerly served as a diplomat in Morocco, was also targeted with spyware but no successful infection took place. It has been reported that the Moroccan Government could potentially be responsible for this targeting. However, that information has not been confirmed[596].

331. Out of the 65 cases, 18 cases have been confirmed to have been targeted by the Spanish authorities, but the government has not commented on the 47 remaining persons[597]. It remains unclear whether or not the other individuals were targeted by the CNI with a court order or whether or not another authority had received court orders to legally target them. Despite the court warrants for the use of spyware on 18 persons, they were not subsequently charged with a crime relating to the warrant authorising the use of spyware. Among the targets for whom surveillance had been authorised are the current President of Catalonia Pere Aragonès, former President and current MEP Carles Puigdemont, and other pro-Catalan independence politicians and associates[598]. Subject to the requirements of secrecy and confidentiality contained in the law, Minister for Defence Robles has referred to the Official Secrets Act for not expanding on the reasons for the surveillance of those specific targets[599]. Most of the 65 Catalan targets have at some point in time been in contact with the members of the pro-Catalan independence movement living outside of Spain. Some of the persons targeted were outside Spain when the infection took place, among other places in Belgium, Switzerland, Germany and France. Such digital surveillance would be illegal in Germany, unless expressly permitted by the federal authorities.

---

[592] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at p. 5.
[593] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.
[594] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7 May 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 May 2022.
[597] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.
[598] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , 5 May 2022.
[599] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html 5 May 2022.

332. One of the key groups revealed to have been targeted is the pro-independence Catalan Members of the European Parliament. Each of them were hacked with spyware either directly or indirectly through what Citizen Lab refer to as relational targeting[600]: Diana Riba i Giner, Jordi Solé, Carles Puigdemont and Clara Ponsati. The mobile phone of a former accredited assistant of Ms Ponsatí was successfully infected with Pegasus. In the case of Antoni Comín, who during a hearing of the PEGA Committee accused the Spanish state of having spied on him, Citizen Lab acknowledged that the infection had been misattributed owing to an error in the labelling of initials.

333. The phone of Diana Riba i Giner MEP of Esquerra Republicana de Catalunya (ERC) was directly infected with Pegasus spyware on 28 October 2019, only three months after taking her seat in Parliament. While in a discussion with her assistant over the phone, the communication was interrupted and her staff member heard a recording of the conversation she just had with Riba i Giner. The timing of this infection directly coincided with a crucial court ruling on the Catalan separatists, one of whom is Raül Romeva, husband of Riba i Giner who ultimately received a 12-year sentence[601]. Riba i Giner outlined at a hearing of the PEGA Committee in Parliament that, at that time, the majority of her phone calls related to the court case, as well as carrying out countless meetings and visits to the courts. As such, the by-catch in this instance was incredibly significant, including Romeva and those connected to the landmark case[602].

334. Jordi Solé MEP, also of the ERC, was originally reported to have been hacked on both the 11and 27 June 2020 according to the research of Citizen Lab[603]. However, five further attacks during the same period were later discovered[604]. Solé only discovered that he had been targeted with Pegasus by accident when, after receiving some potentially suspicious messages, he submitted his phone to be checked as part of a documentary[605]. Similarly to the case of his colleague, the timing of this targeting is worthy of note. It came during critical political discussions on the vacant seat of Oriol Junqueras, who was not granted permission to take up his position as an MEP while imprisoned in Spain[606] and only one month before Solé was appointed to take over the seat in July 2020. Moreover, there were ongoing discussions at that time on party strategy and international litigation regarding their imprisoned and exiled colleagues during the time of the infections[607].

335. Carles Puigdemont, MEP for JUNTS and former President of Catalonia, was targeted

---

[600] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at p.6.
[601] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing, testimony of Ms Diana Riba i Giner MEP, Strasbourg, 6 October 2022.
[602] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing, testimony of Ms Diana Riba i Giner MEP, Strasbourg, 6 October 2022.
[603] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at p. 7.
[604] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing, testimony of Mr Jordi Sole MEP, Strasbourg, 6 October 2022.
[605] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , 18 April 2022.
[606] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing, testimony of Mr Jordi Sole MEP, Strasbourg, 6 October 2022.
[607] Politico, https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/, 9 January 2020.

through his spouse Marcela Topor, members of staff and a number of his associates[608]. In total, Citizen Lab report that up to 11 individuals in close contact with Puigdemont were targeted, including at least two confirmed infections on Topor's device on 7 October 2019 and 4 July 2020[609].

336. Clara Ponsatí, MEP for JUNTS and former Minister of Education of Catalonia, was a relational target. Pol Cruz, a staff member at the European Parliament, was confirmed to have been infected on 7 July 2020[610].

337. All of the Presidents of Catalonia since 2010 have been targeted with spyware either during or after their term in office[611]. As many as 12 ERC members were among the 65 targets, including the Secretary General of the party, Marta Rovira, who was hacked at least twice in June 2020 according to Citizen Lab. It is highly significant that both Gabriel and Rovira were living in Switzerland at the time of their surveillance, following the fallout in the wake of the 2017 referendum.

*CIVILIAN TARGETS, INCLUDING JOURNALISTS, LAWYERS AND CIVIL SOCIETY REPRESENTATIVES*

338. Jordi Domingo was one of the first Catalonian activists who was reported to have been targeted in 2020. Though a supporter of Catalan independence and member of the Catalan National Assembly (ANC), it was reported by *The Guardian* that Domingo believed himself to be a mistaken target. Given that he did not play a major role in the events of 2017, it is his belief that the intended target was a lawyer of the same name who contributed to the drafting of a potential constitution for an independent Catalonia[612].

339. The ANC, a Catalan civil society organisation supporting Catalan independence, was one of the first organisations targeted prior to the Catalan referendum, and has since been subject to extensive targeting[613]. The six targets of the ANC include two of its former presidents, Jordi Sanchez (2015-2017) and Elisenda Paluzie (2018-2022), whose spyware surveillance was granted by court order, as was that of the expert in digital voting and decentralisation, Jordi Baylina, two members of its National Board (Arià Bayè and Sònia Urpí) and one member of a local branch (Jordi Domingo).

340. The devices of individuals close to Jordi Cuixart, president of Òmnium Cultural (until February 2022) were infected, as he was imprisoned at that time. These included Marcel Mauri, serving as a Vice-President of the NGO, whose spyware surveillance was granted by court order.

---

[608] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at p.7.
[609] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022 at p.8.
[610] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ 18 April 2022 at p.7.
[611] Artur Mas (after leaving office), Carles Puigdemont (relational targeting), Joaquim Torra (while in office), Pere Aragones (infected while serving as Torra's Vice-President). https://catalonia.citizenlab.ca/.
[612] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware, 13 July 2020.
[613] Citizen Lab's CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

341. Citizen Lab discovered an active Candiru infection on the laptop of Joan Matamala, a businessman and activist with close ties to pro-independent Catalan politicians, in February 2021[614]. Matamala's spyware surveillance was granted by court order. Candiru is significantly harder to trace than Pegasus, and this discovery of an active infection allowed the researchers at Citizen Lab to better understand its patterns. Subsequently, 16 other infections on Matamala's device were discovered[615]. Microsoft subsequently patched the vulnerabilities through updates, but it is impossible to know the number of Candiru infections that have gone unnoticed[616].

342. At least three renowned open source developers and entrepreneurs were targeted with Pegasus. Xavier Vives and Pau Escrich, co-founders of Vocdoni, an Ethereum blockchain-based open source protocol for secure, censorship-resistant digital voting, were both targeted. Vives was specifically targeted with the Candiru malware, whereas Escrich was targeted with both Pegasus and Candiru[617]. Vives and Escrich's spyware surveillance was authorised by a court order.

343. Gonzalo Boye is the lawyer of former Presidents Puigdemont and Torras[618]. During the five months between January and May of 2020, Boye was targeted as many as 18 times via text messages that appeared as tweets from civil society organisations or prominent news outlets[619]. Citizen Lab confirmed at least one successful infection on 30 October 2020. The infection came just 48 hours after the arrest of one of his clients[620]. The targeting of Boye has called into question the legality of attacking lawyer-client privilege.

344. Elena Jimenez, the International Representative of Òmnium Cultural, and Jordi Bosch, the lawyer responsible for Institutional Relations of Òmnium Cultural, were both targeted with Pegasus while serving on the legal team of Jordi Cuixart. Jimenez was in constant contact with Cuixart's full legal team, including the international team who were preparing a complaint to the ECtHR. So far, Citizen Lab have only examined Jimenez's most recently acquired mobile phone, but they confirmed a successful zero-click infection in February 2020. Bosch, a less public face of the legal team, was targeted in July 2020, less than a week before Cuixart was granted a more lenient form of detention and on the same day as he appeared on Catalan television on behalf of Òmnium for the first time.

345. Andreu van den Eynde i Adroer was successfully infected with Pegasus on 14 May 2020[621]. The hacking occurred while he was acting as the lawyer of both Raul

---

[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.
[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 at p.10.

Romeva and Oriol Junqueras in their case before the Supreme Court.

346. Similarly, lawyer Jaume Alonso-Cuevillas' device was also infected while representing key Catalan figures such as Carles Puigdemont. However, Citizen Lab were unable to determine the precise date of the successful infection.

INVESTIGATIONS AND LEGAL REFORMS

347. After the allegations contained in the 'Catalangate' case came to light on 22 April 2022, the Spanish institutions began a process of scrutiny aimed at ensuring that the guidelines on surveillance had been applied correctly. These measures involved the summoning of Paz Esteban, Director of the CNI, before the Official Secrets Committee on 5 May, announced by Minister of the Presidency Felix Bolaños; the session of parliamentary scrutiny of the government and the Minister of Defence on 26 and 27 April; and the independent assessment conducted by the Ombudsman, which was launched on 26 April 26 and concluded on 18 May. Minister of Defence Margarita Robles, while bound by secrecy in accordance with the Official Secrets Act, hinted at the fact that the measures had been taken in response to the action of those who 'violate the Constitution, take over public infrastructure, create public disorder and [those who] have ties with the political leaders of a country who is invading Ukraine'[622]. The government party (PSOE) and the three main opposition parties (PP, Vox and Ciudadanos) reported that the director had provided satisfactory explanations on the necessity and legality of the spyware surveillance measures[623] [624].

348. The Spanish Ombudsman concluded that much of the surveillance conducted in Spain by the CNI was done in full respect of the legal procedures. Following his recommendations on the adequacy of parliamentary and judicial controls, and in order to update the legislation, reinforce the guarantees of judicial control and ensure maximum respect for the fundamental rights of individuals, the Spanish executive committed to:

1. issue an internal investigation within the CNI;

2. launch an investigation within the committee on the use and control of credits allocated to secret funds of the Spanish Congress and hold a hearing where the Director of the CNI would appear; and

3. the disclosure to the committee on the use and control of credits allocated to secret funds of the Spanish Congress of the Supreme Court; 18 orders authorising the intrusions; and the declassification of CNI documents relating to the targeted pro-Catalan independence movement members, on request of a judge;

[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 May 2022.
[624] El Periodico de Espana, https://www.epe.es/es/politica/20220505/frente-comun-pp-vox-cs-13614030, 5 May 2022.

4. the reform of the 1968 Spanish Law on Official Secrets[625];

5. the reform of the legal framework of the CNI[626];

6. the approval of a new Intelligence Directive, setting the CNI's intelligence objectives; and

7. update the 2021 national security strategy and the cybersecurity plan.

349. Spain's High Court[627] opened its own investigation after the government stated that Pegasus software had been used to spy on ministers, including Prime Minister Sanchez. As part of a so-called investigative commission to investigate the spying, the court called the chief executive officer of Israel's spyware software Pegasus firm NSO Group and Minister Felix Bolaños to testify as witnesses. The investigative judge also interviewed former Director of the National Intelligence Centre, Paz Esteban[628] [629], as well as the Defence and Interior Ministers, whose devices were among those hacked. The Court[630] sent a formal request for international judicial assistance to the Israeli Government asking for information on 'different aspects of the software tool'. The High Court also lifted the secrecy of the documents related to the case and overturned a ban on investigating the wiretapping of mobile phones belonging to Prime Minister Pedro Sánchez and Defence Minister Margarita Robles.

CONCLUDING REMARKS

350. Spain has an independent justice system with sufficient safeguards. However, following the discovery of the two categories of targets in Spain, some questions remain, which could be answered by swift and profound reforms and their effective implementation. The Spanish Government is working on modifications to address shortcomings. On the CNI reform, the Spanish Government announced its intention on 26 May 2022 to reform the legal framework of the CNI, but no proposal has been submitted yet. On 1 August 2022[631], the government submitted legislative amendments to the Official Secrets Law. The government is currently awaiting the opinion of the Council of State.

351. The 47 targeted persons mentioned in the Citizen Lab report, for whom it remains unclear whether or not they were targeted by the CNI with a court order, or whether or not another authority had received court orders to legally target them, do not know the reasons, scope or actors behind the targeting with Pegasus. These persons should have

[625] El País, 'El Gobierno inicia la reforma de la ley franquista de secretos oficiales', 5 April 2021.
[626] La Moncloa, 'Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías', 26 May 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.

access to justice and an investigation should be launched in order to shed light on these cases.

352. With regard to the 18 cases for which a court order had been issued, their legality has been verified and confirmed by the Ombudsman, but their special nature, adequacy, exceptional nature, proportionality and necessity[632] can only be verified by a court.

353. More generally, judicial proceedings by the individuals targeted are not going as quickly as hoped for, with the aim of providing transparency and access to meaningful legal remedy. Cooperation by the authorities is crucial here. In order to provide greater clarity and contribute with technical expertise, Europol could be invited and could provide support to ensure that a proper forensic process is followed.

*I.F. Other Member States*

THE NETHERLANDS

354. The 2017 coalition agreement of the Dutch Government states that the Dutch police are not allowed to acquire spyware from providers that provide their products to 'dubious regimes', later specified as 'countries guilty of grave violations of human rights or international humanitarian law'. Before any acquisition of spyware, the Dutch police have to ask the provider whether it has provided spyware to countries which have been sanctioned either by the EU or by UN and carry out a check on whether the country where the provider is based has an export control regime in which human rights are assessed in the export license procedure. This assessment is repeated periodically. It should be noted that this restriction only seems to apply to spyware acquisitions by the police. The intelligence services are not explicitly mentioned. According to the government, the police have been using hacking software since 2019, although the authorities do not mention which type[633]. It would appear that the NSO Group and its spyware product Pegasus do not meet the abovementioned standards, in any case not before the tightening of the export regime of Israel in December 2021[634]. No insight has been given into the expenditure by both police and intelligence services for the purchase and use of the spyware system.

355. In the Netherlands, a new body (Toetsingscommissie Inzet Bevoegdheden, TIB) became operational in 2018 to assess in advance the legality of the authorisation by the government to the intelligence agencies to employ surveillance techniques. Surveillance cannot proceed if the TIB deems the authorisation unlawful. The TIB supplements the main oversight body, the Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD). CTIVD supervises ongoing surveillance activities by intelligence services after the authorisation has been granted and handles complaints.

356. It should be noted that from November 2014 to December 2016, NSO Group was able to operate thanks to two companies, Shapes 1 BV and Shapes 2 BV, established in the

[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.

Netherlands, in the ‘financial holdings’ and ‘engineers and other technical design and advice’ sectors. Both were liquidated after two years in operation[635].

357. On 4 October 2022, it was revealed that in November 2019 the Dutch Ministry of Defence was about to sign an agreement with WiSpear, the company owned by Tal Dilian, which had earlier acquired Cytrox, the manufacturer of Predator spyware[636]. WiSpear had won a tender issued by the Dutch Ministry. It does not emerge clearly from the email exchange whether it concerns Predator or another product. From disclosed emails exchanged between the Cypriot Ministry of Energy, Commerce and Industry and WiSpear, it becomes clear that a representative of the Dutch Ministry of Defence had contacted the Cypriot Ministry of Commerce to obtain assurances about WiSpear on 13-15 November 2019, only days before the Dilian ‘spy van’ story broke. Dilian informed the representative of the Cypriot Commerce Ministry that he would appreciate her immediate assistance in the matter, as the as the deadline for signing the contract signatures was approaching’[637]. It is not clear whether or not the contract was signed and any spyware was provided to the Dutch Ministry of Defence.

358. The Netherlands is also home to a subsidiary of Cognyte registered as Cognyte Netherlands B.V. As seen in an excerpt from the Dutch Chamber of Commerce, the sole shareholder of the Dutch subsidiary is Cyprus-based UTX Technologies. As described in the chapter on ‘Cyprus and the Spyware Industry’, UTX Technologies has a history of exporting intelligence and tracking systems to Bangladesh and shipping monitoring systems to EU Member States. In addition, the Israeli company Verint – which also owned Cognyte before its spin-off in 2021 – was the main supplier of the monitoring system to the Dutch police[638]. The connections between the police and this Israeli supplier become even clearer once we observe that former police officer Robert van Bosbeek has taken on the role of director of Cognyte Netherlands B.V. since 2014[639]. Another director of this Dutch subsidiary, David Abadi, is also the chief financial officer of Israeli Cognyte Software Ltd, which has been linked to the sale of interception spyware to Myanmar[640].

359. On 2 June 2022, the media reported that the Dutch intelligence service Algemene Inlichtingen- en Veiligheidsdienst (AIVD) used Pegasus when it assisted the police in tracking down a suspect in a serious crime, Ridouan T, who became a prime suspect in multiple murders related to organised crime, drug trafficking and leading a criminal organisation, and was arrested on 16 December 2022 in Dubai[641]. The Dutch Government refused to comment. This is a remarkable case that merits closer attention. The leaks took place at a time when Pegasus and the NSO Group were attracting a lot of public criticism, and the blacklisting by the US Department of Commerce hurt the NSO Group financially. The Dutch success story of catching an individual who had been one of the most wanted criminals in years was a welcome positive message for the

[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’.
[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/.

company. The media report is based on statements by four sources within the AIVD. Their motive for the leak is not mentioned in the report. Nor does there seem to have been an investigation into these leaks, which raises the question as to whether the leak had the approval of the AIVD's management. It is, however, highly unlikely that the AIVD would allow such a story to get out without the knowledge and approval of the Israeli authorities.

BELGIUM

360. In an interview with *The New Yorker*, a former Israeli intelligence official revealed that the Belgian police uses Pegasus in its operations[642]. In response, the Belgian police stated they would 'not communicate about any technical and/or technical means used for investigations and missions'. In September 2021, Minister of Justice Vincent Van Quickenborne mentioned that Pegasus 'can be used in a legal way' by the intelligence services, but did not want to confirm whether the Belgian intelligence service is a client of NSO or is using any spyware against criminals[643].

361. El Mahjoub Maliha, human rights defender from the Western Sahara, based in Belgium, and Carine Kanimba, daughter of Rwandan political activist Paul Rusesabagina, have also been spied on via Pegasus software while in Belgium, and even during meetings with Belgian Government officials. The spyware attacks were most likely carried out by, or on behalf of, the Moroccan and the Rwandan authorities respectively. Rwanda also stands accused of using Pegasus spyware to target critics living in Belgian exile, including prominent opposition figures Placide Kayumba and David Batenga[644]. The Belgian military intelligence service ADIV further discovered that Pegasus had very likely been installed by Rwanda on the smartphone of Kagame-critical Belgian journalist Peter Verlinden and his wife Marie Bamutese[645]. Other Belgian targets of the use of spyware include former PM Charles Michel and his father Louis Michel (then MEP, former Commissioner and Foreign Minister). According to the Belgian media, the Moroccan Government was behind the attacks[646].

GERMANY

362. German entities that make and have made use of hacking are the Bundesnachrichtendienst, the Federal Intelligence Service or BND, the military and the customs and police services. The BND is the agency which makes the greatest use of hacking. In 2009, they had already monitored 2 500 devices[647].

363. A legal framework regulating the use of spyware is in place in Germany. Since 2008, German federal law has granted state hacking powers to the police in cases of

---

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.
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.

international terrorism and for the prevention of terrorist attacks[648]. In 2017, a new law came into force, allowing every law enforcement agency to use state hacking in the case of 42 criminal offences. These offences include the submission of fraudulent asylum applications, tax evasion and drug offences, among others[649]. In 2021, the Bundestag adopted the Federal Government's draft law 'on the adaptation of the law on the protection of the constitution'. This change legalises state hacking for all 19 German intelligence agencies[650] and stipulates the obligation for communication providers to cooperate with the state in hacking activities[651].

364. Hacking laws in Germany are often justified in the light of cases of crimes against sexual self-determination, child pornography, the formation of criminal organisations and murder. However, most of the investigations in which the police have used hacking tools were unrelated to the abovementioned crimes[652]. The most recent figures from 2020 show that the German police received authorisation for 48 hacks. They only used 22 hacks, of which none were related to fighting terrorism and murder[653].

365. In September 2021, it was reported that the German Federal Criminal Police Office (BKA) had acquired Pegasus in late 2020. It is important to note here that German law distinguishes between two forms of spyware use[654]: access to all information (Online-Durchsuchung[655]) and access to only live communication (Quellen-TKÜ[656]). Since the original Pegasus software could access all information on a device, and not just live communication, its use by the BKA would break the law. Since a landmark ruling of the German Federal Constitutional Court in 2008, any spyware used by police authorities has to comply with the standards for telecommunication and online surveillance set up for the BKA [657] [658]. The BKA therefore asked NSO to write a source code, so that Pegasus would only be able to access what was allowed by law. Initially, NSO declined to do so[659]. Only after new negotiations, did NSO agree, so the BKA acquired a modified version[660]. While this has not been acknowledged publicly, Martina Link, then Vice-President of the BKA, confirmed the purchase of a modified version during an in

[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.
[653] The Quellen-TKÜ (§ 100a StPO) was approved 25 times and executed 14 times, and Online-Durchsuchung (§ 100b StPO) approved 23 times and executed 8 times. Data retrieved from: 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.

camera meeting of the Innenausschuss in the Bundestag[661]. It has allegedly been deployed since March 2021. The version purchased by the BKA had certain functions blocked to prevent abuse, although it is unclear how this works in practice. The BKA has written a report about this modified version, which remains classified[662]. The BKA denied civil society organisations access to the contracts with spyware companies until they were forced to do so by court. However, even then, they only released the contracts in heavily redacted versions[663]. Despite two invitations to the PEGA Committee, the BKA has not been able to attend any hearings owing to scheduling issues.

366. In October 2021, it was also revealed that the German foreign intelligence service, the Federal Intelligence Service (Bundesnachrichtendienst, BND), had bought a modified version of Pegasus, although the acquisition was classified[664]. In response to a parliamentary question, the Federal Government indicated that the use of Pegasus is only permitted in individual cases and must comply with the strict legal conditions laid down in the German Code of Criminal Procedure (StPO), the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (G-10 Act) and the Federal Criminal Police Office Act (BKAG), but it could not comment further on its use owing to reasons of secrecy (Geheimhaltungsbedürftigkeit)[665].

*USE OF SPYWARE*

367. In 2012 and 2013, both the German Federal Police BKA and Berlin Police LKA independently purchased FinSpy from FinFisher. Here too, just as in the case of Pegasus, the BKA told the company to develop the FinFisher spyware in such a way that it could not access all data on a device, but only live communications, for it to be compliant with German law. The BKA kept testing new versions of the spyware provided by FinFisher for it to be used only in a 'legally secure and technically clean' manner, and only after five years, in 2018, did the Federal Ministry of the Interior approve its use. This was during the same year as the use of FinFisher software against opposition parties in Türkiye was discovered, whereas Germany had not issued any export license for exports of surveillance software to third countries since 2015[666]. However, the contract between FinFisher and the Berlin Police had already ended by then, so the police in the capital never used it. The BKA did not comment further on any use of FinFisher in its operations or on whether the contract is still valid[667].

368. In 2017, the Federal Minister of the Interior launched the Central Office for Information Technology in the Security Sector (ZITiS) for the facilitation of research and development for hacking tools by the government, as well as the purchase of hacking

---

[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/.

[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/.

tools from commercial vendors[668]. On 6 April 2022, it was reported that ZITiS was prospecting for available technologies elsewhere in the wake of the disgraced spyware company Finfisher's filing for bankruptcy[669]. Among other things, it was reported that, since 2019, it had met five times[670] with the Italian surveillance company RCS Lab, but there was no proof of the acquisition of a tool from RCS lab[671]. In addition, ZITiS met and evaluated spyware products of the Austrian firm DSIRF[672] and the Israeli firms Quadream[673] and Candiru[674].

369. In January 2023, *Tagesschau* reported that ZITiS was also in contact with Intellexa or its subsidiary Cytrox, although it is unclear whether the Predator spyware was eventually purchased. Former secret service coordinator Bernd Schmidbauer reportedly acted as a representative for Intellexa's products. According to emails from November 2021, Mr Schmidbauer was in contact with the former President of the Federal Office for Information Security Arne Schönbohm, aiming to arrange an appointment with Intellexa. In February 2022, Mr Schmidbauer also contacted the President of ZITiS for a presentation of Intellexa. In addition, Mr Smidbauer was in touch with the Vice-President of the Federal Office for the Protection of the Constitution (BfV), which reportedly resulted in a presentation of Intellexa to personnel of the BfV at the beginning of July 2022. The government did not comment on the appointments resulting from the controversial lobbying activities of Mr Schmidbauer[675]. In 2021, Mr Schmidbauer had also met Jan Marsalek, who is connected to DSIRF[676].

MALTA

370. Several key figures from the spyware trade have either registered a business on Malta or have obtained Maltese passports, but it appears they do not actually reside there, nor do their companies appear to be active. A few key personalities from the spyware trade have been identified so far.

371. Tal Dilian is an Israeli citizen, formerly of the Israeli army. He is a founder of Intellexa and lives in Cyprus. He acquired a Maltese passport in 2017[677]. He also co-owns a company on Malta called MNT Investments LTD[678].

372. Anatoly Hurgin is a Russian-Israeli citizen and former Israeli military engineer. He

---

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/.
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/.

acquired a Maltese passport in 2015[679]. He is the founder of Ability Ltd, which cooperated with NSO Group on Pegasus and handled the network side of NSO's operations[680]. At the time of his application for a Maltese passport, he was already under investigation by both the US and Israeli authorities for various crimes[681]. Investigative journalist Daphne Caruana Galizia, who was later murdered in October 2017, wrote about him in August 2016[682]. In 2017, Ability Ltd was under investigation by the US Securities and Exchange Commission for allegedly lying about the state of its finances and it was also almost delisted by NASDAQ[683]. Mr Hurgin reportedly also owns a company in Lithuania called UAB 'Communication technologies' which provides 'connection and telecommunication services'[684].

373. Felix Bitzios is Director of Malta-based company Baywest Business Europe Ltd[685], was formerly an owner and employee of Intellexa and was involved in the Piraeus/Libra fraud case[686];

374. Stanislaw Szymon Pelczar is legal representative of Baywest Business Europe Ltd, registered in Malta, and was a former administrator at Krikel. He was mentioned in the Paradise Papers[687];

375. Peter Thiel is a German-born American citizen who acquired New Zealand citizenship in 2011 despite not residing there. He applied for a Maltese golden passport in 2022 (shortly after the announcement of the joint start-up of Mr Kurz and Mr Hulio)[688]. He is a founder of PayPal and of the controversial company Palantir (connected to the Cambridge Analytica scandal). He is a sponsor of Donald Trump and the first outside investor of Facebook. He hired Sebastian Kurz (who recently founded a business with Shalev Hulio, ex-NSO) as strategist[689];

FRANCE

*TARGETS IN FRANCE*

376. In 2021, the Pegasus Project revealed several cases of attempted hacks by the Pegasus

[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/.
[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/.

spyware in France[690]. The leaked dataset included the telephone number of President Emmanuel Macron, as well as the telephone numbers of 14 members of his cabinet[691] [692]. The findings of forensic analyses by the French state intelligence services have confirmed that the telephones of Minister of Education Jean-Michel Blanquer, Minister of Territorial Cohesion Jacqueline Gourault, Minister of Agriculture Julien Denormandie, Minister of Housing Emmanuelle Wargon and Minister of the Overseas Sebastien Lecornu were infected with the Pegasus spyware[693]. The telephone of Member of Parliament Adrien Quatennens was also infected[694].

377. The register as seen by the Pegasus Project reportedly also contained the telephone numbers of other French citizens, among them journalists, former politicians and their relatives. Pegasus infections of mobile devices belonging to the director of Parisian radio station TSF Jazz Bruno Delport, former minister Arnaud Montebourg and investigative journalists Edwy Plenel, Lénaïg Bredoux and an unnamed journalist from France 24 have been confirmed by France's computer security agency (Agence nationale de la sécurité des systèmes d'information)[695]. In addition, Claude Mangin – wife of Naâma Asfari, a Saharawi political prisoner in Morocco – was also targeted with Pegasus[696]. Furthermore, the Paris-based defence lawyer of several Polisario Front activists for the Sahara cause, Joseph Breham, was also targeted with Pegasus[697].

378. Morocco seems to be behind many of the attacks on both journalists and politicians in France[698], including Moroccan journalists living in French exile, in particular the investigative journalist Hicham Mansouri, who fled the Moroccan authorities' continuous harassment in 2016, and the independent journalist Aboubakr Jamai, who left Morocco in 2007[699].

379. Reportedly, France was about to purchase Pegasus spyware itself in 2021. At the time of the final negotiations with NSO Group, revelations about the spyware allegedly being used against French Government officials led to the abrupt suspension of the sale[700]. The French Ministry of Foreign Affairs has denied holding talks with NSO Group[701].

380. In a PEGA Committee meeting on 9 January 2023, Serge Lasvignes, Chair of the National Committee for the Control of Intelligence Techniques, stated that the decision to not authorise the use of Pegasus in France was taken before the revelations by the Pegasus Project. According to Lasvignes, the French intelligence services only make

---

[690] The Guardian, Pegasus spyware found on journalists' phones, French intelligence confirms.
[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.

use of surveillance products that are created in France so as to avoid foreign spyware producers obtaining access to information. However, Lasvignes specified that the technical directorate that builds the French spyware does in fact import certain parts from non-French companies[702].

381. In France, requests for the authorisation of surveillance of a person have to be approved first by the Director-General of the service, then by the Minister of the Interior. Ultimately, all requests must be authorised by the Prime Minister. Currently 23 000 people are under surveillance in France, and each operation has been authorised by the Prime Minister. If a target wishes to inquire whether they are or have been under surveillance, access to their files is denied with reference to national security. The person may request verification by a judge. However, the judge can only decide whether or not the surveillance was legal, but cannot inform the target since this comes under national security confidentiality[703]. This means that, in practice, the right to legal redress is meaningless, as the burden of proof lies with the individual and it is virtually impossible to obtain any proof from the authorities.

382. According to an ISS World Brochure from 2013, the French Ministry of the Interior, the Ministry of Defence, Interpol and the Embassy of Togo in France were all present at the ISS World 2012, also known as 'The Wiretappers' Ball', as attendees. In addition, a list of ISS vendors and technology integrators shows that the following French spyware companies were present at this event: 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 and WAHOUE AND PARTNERS[704].

*SPYWARE COMPANIES IN FRANCE*

383. France is home to different spyware companies, of which the most eminent are Nexa Technologies and Amesys. Nexa technologies, part of Tal Dilian's Intellexa Alliance, is a French cyber defence and intelligence company, established in 2000[705]. Nexa Technologies is run by former managers of Amesys. Amesys was founded in 1979[706] and is known for the sale of a program called Cerebro, capable of tracking the electronic communications of its targets, such as email addresses and telephone numbers[707].

384. In 2007, Amesys reportedly sold this telecommunication surveillance technology to Libya, which was used by the Gaddafi regime to arrest and torture critics of the regime. According to *Telerama*, Nexa was founded to rebrand the surveillance software and to continue the sales of Amesys to the Egyptian regime[708]. In 2014, Nexa Technologies allegedly sold an interception system to the Egyptian regime under the name Eagle. This system was used in connection with the detention and torture of political opponents

[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.
[708] ZDNet, Amesys and Nexa Technologies executives indicted.

of the Al-Sissi regime[709]. Eagle was deployed and maintained by Amesys from 2007 to 2011[710].

385. Several complaints have been filed against both Amesys and Nexa Technologies. In October 2011, the International Federation for Human Rights (FIDH) and Human Rights League (LDH) filed a lawsuit against Amesys at the Paris High Court in the light of their alleged sales to Libya[711]. Five Libyan targets were heard in the summer of 2013 and one Libyan target was heard in December 2015. As a result of new evidence underlining the use of Amesys' surveillance technology by the Gaddafi regime, Amesys was officially assigned the status of assisted witness for complicity in torture between 2007 and 2011[712].

386. In 2010, Amesys was taken over by French computer firm Bull. In 2014, Atos, led at the time by Thierry Breton, took over Bull and therefore also acquired Amesys[713]. At the time of the takeover, the dubious activities of Amesys in terms of trade with authoritarian regimes were already well known. Indeed, a complaint had already been lodged.

387. In 2017, an investigative media report revealed the sale of surveillance systems by Nexa Technologies to Egypt in 2014, triggering a complaint by FIDH, LDH and the Cairo Institute for Human Rights Studies (CIHRS) against the company[714] [715].

388. In June 2021, following several complaints by human rights organisations, the Paris Judicial Court indicted four executives of Amesys and Nexa Technologies over the sale of surveillance technology to the governments of Libya and Egypt[716]. It is worrying that a whole 10 years had passed between the first complaint and the start of the court case. Meanwhile, Amesys was able to continue its activity unhampered, including the abovementioned sale of surveillance technology to Egypt.

389. Despite these controversies, the French Agence Nationale des Titres Sécurisés (ANTS) signed a contract with Amesys in October 2016 worth over EUR 5 million for the technical management of the TES database (containing the personal data and biometrics of all French citizens). This decision of the French authorities to involve Amesys, then already known for its practices, in such a project was subject to criticism. While Amesys would not be in full control of the systems used for the controversial TES database file, it would assist the agency's project managers who deal with the TES file, so it cannot be excluded that Amesys would have access to personal data. However, the Director of ANTS considered that there was no legal objection to conducting business with Amesys[717].

---

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

390. In France, the provision of export licences is controlled by the Dual-Use Goods Service (SBDU) of the Ministry of the Economy, Industry and Digital Affairs. In addition, the Inter-Ministerial Commission on Dual-Use Items – chaired by the Ministry for Europe and Foreign Affairs – inspects the more sensitive dual-use items. At the time of writing, no information on the granting of export licences by the French Government to Nexa Technologies was available.

IRELAND

391. Ireland has become the Member State where some of the main spyware companies involved in scandals have registered, owing to its fiscal laws. On 20 September 2022, *The Currency*, an Irish investigative journalism publisher, revealed that both Thalestris Limited, the parent company of Intellexa, and Intellexa itself are headquartered in Ireland, and registered at a law firm in the town of Balbriggan. It is remarkable that the application to incorporate Thalestris Limited in Ireland was submitted in November 2019 by a company formation specialist, only 12 days after the criminal investigation into Dilian and his company WiSpear by the Cypriot authorities was publicly revealed. Tal Dilian himself, CEO of Intellexa, does not appear on Irish company documents, but his second wife Sara Hamou is reportedly named as director of both Thalestris and Intellexa[718].

392. Published accounts by Thalestris for the period ending on 31 December 2020 indicate that 10 other subsidiary companies exist in Greece, Cyprus, Switzerland and the British Virgin Islands, and that Thalestris was not liable to pay any corporation tax. It used a number of fiscal provisions also used by multinationals operating in Ireland and was therefore technically loss-making[719].

393. The Irish Government refused to respond to the question as to whether it or any law enforcement agencies had been approached by Thalestris or Intellexa, or if they had ever used their services, arguing that ‘for sound operational and national security reasons it would not be appropriate to comment on the details of national security arrangements, nor would it be appropriate to disclose the department’s cyber security arrangements or those of state offices, agencies and bodies under the department’s remit’. The Irish Government also refused to comment on any Irish links to the spyware produced by Thalestris and Intellexa[720]. There is no publicly known evidence of abuse of spyware in Ireland.

394. *Haaretz* revealed that a firm called GoNet Systems, which was involved in providing Wi-Fi infrastructure services at Larnaca Airport, and which was linked to Dilian’s

[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/.

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

WiSpear and shut down in 2022, also had corporate ownership in Ireland[721].

395. In January 2023, it was reported that the Oireachtas Committee on Justice was to examine the existence of companies in Ireland involved in the production of spyware following a letter sent by MEP Barry Andrews. The committee stated that it had considered the matter during a private meeting on 18 January and agreed to add the topic to its work programme for 2023[722].

396. It must be noted that Irish corporate law is kept under ongoing review and updated on a regular basis, in order to increase the transparency of business structures. Examples include the Companies (Corporate Enforcement Authority) Act 2021, which updated the enforcement regime, and an upcoming update thereof expected in 2023, and the Miscellaneous Provisions (Transparency and Registration of Limited Partnerships and Business Names) Bill 2023. Furthermore, the Irish Government indicated further investments in the National Cyber Security Centre (NCSC) in order to increase the NCSC's ability to actively detect and defeat cyber threats targeting critical infrastructure and critical networks through a variety of means. The ability of the NCSC to monitor and respond to incidents will be developed through the ongoing evolution of the Joint Security Operations Centre (JSOC) and expanded analytical and reporting capabilities. Work is also progressing on the development of a technology strategy for the NCSC with external consultants[723].

LUXEMBOURG

397. Luxembourg hosts nine entities directly related to NSO Group, as was revealed by Amnesty International in June 2021 and confirmed by the Luxembourgish Foreign Affairs Minister Jean Asselborn[724]. The fact that the names of the nine companies (such as Triangle Holdings SA, Square 2 SARL, and Q Cyber Technologies SARL), all under the umbrella of management and private equity firm Novalpina Capital, do not immediately reveal the connection with NSO Group, shows how opaque business structures in Luxemburg allow companies to operate completely out of the public view in Luxembourg.

398. Following Amnesty's revelations about the nine NSO entities in Luxembourg in June 2021, Foreign Minister Jean Asselborn sent each of them a letter, calling on them to refrain from any decision-making that could lead to an illicit use of the goods and technologies that they make available to their customers. According to LuxTimes, NSO Group replied that it only exports its spyware from Israel with the consent of the Israeli Government, but Asselborn stated in October 2021 that he could not verify that[725]. In any case, according to the minister, none of the nine entities was authorised to export cybersurveillance products from Luxembourg, as Luxembourg has not granted any

[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.
[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.

export licences[726]. ‘Luxembourg will not, under any circumstances, tolerate export operations from Luxembourg contributing to human rights violations in third countries and will ensure, if applicable, to take the necessary measures to remedy any violation of human rights and to prevent future violations’, said Asselborn[727]. However, NSO Group is still able to operate thanks to the entities based in Luxembourg, such as Q Cyber Technologies, which is responsible for handling invoices, contracts and payments from customers of its software[728]. On 24 August 2022, it was revealed that NSO Group had booked more than half of its sales over the two previous years in Luxembourg, making clear that Luxembourg functions as an important business hub for NSO Group[729].

399. In October 2021, Prime Minister Xavier Bettel confirmed that Luxembourg bought and used Pegasus ‘for reasons of state security’[730].

ITALY

400. So far, there have not been any reports on the possible purchase of spyware by the Italian authorities. No high-level cases of spying have been reported, although the telephone number of former Prime Minister and Commission President Romano Prodi was found on the list published by the Pegasus Project[731]. As former UN Special Envoy for the Sahel, he could have been an interesting target for Morocco, considering his possible networking with high-level figures in the Western Sahara and Algeria.

401. Spyware companies Tykelab and RCS Lab have chosen Italy as their base for business.

402. Another company offering offensive intrusion software from Italy since at least 2012 was Hacking Team, now called Memento Labs. The company gained notoriety after a hack which disclosed sales to several authoritarian countries which went on to use the RCS spyware to attack political dissidents, journalists and human rights defenders. An inquiry launched by NGOs and UN investigators into the export of RCS spyware to Sudan eventually led the Italian authorities to impose a ‘catch-all’ provision under Italian export law owing to human rights concerns, and so the company needed to seek individual authorisation for every export. While not only refusing to cooperate during the inquiry, Hacking Team also leveraged its close relationships with senior officials in government, the intelligence services and law enforcement in Italy to position itself as a national security asset, and eventually pressured the Ministry of Economic Development into re-granting them a global licence for export[732].

---

[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.
[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/.

AUSTRIA

403. In response to written questions by the Austrian Parliament, the Austrian Federal Government stated that Austria has not been a client of NSO[733]. However, its former Chancellor Sebastian Kurz has close ties to the founder of NSO Group, and DSIRF, a large spyware provider, is based in Austria.

404. Following his resignation, Mr Kurz was subsequently recruited as global strategist for Thiel Capital, owned by billionaire Peter Thiel[734]. In October 2022, Mr Kurz and Shalev Hulio (founder of NSO Group) launched a cybersecurity firm called Dream Security[735]. Although Mr Hulio had stepped down as NSO Group CEO in August 2022, Dream Security and NSO have close ties through various personal and business connections. One of its investors, Adi Shalev, was also an early investor in NSO. Gil Dolev is another founding member of Dream Security. Dolev's sister Shiri Dolev is the President of NSO Group. Shalev Hulio has previously acquired one of Gil Dolev's companies[736].

405. In July 2022, operators used spyware from Austria-based company DSIRF to hack into law firms, banks and consultancy firms in Austria, Panama and the UK. According to Microsoft researchers, DSIRF's 'Subzero' tool used zero-day exploits to access confidential information, such as passwords and other credentials[737]. In October 2022, the Federal Ministry of Labour and Economic Affairs said it was not aware of any applications for export licences by DSIRF, and that no export applications for 'intrusion software' had been made in the last 10 years[738]. In the absence of an export licence for the export of software by DSIRF, the Vienna Public Prosecutor's Office initiated a preliminary investigation on suspicion of unlawful access to a computer system under Austrian law.

ESTONIA

406. Estonia has reportedly also shown interest in purchasing NSO Group's Pegasus spyware. Initial negotiations between Estonia and NSO Group took place in 2018, following which Estonia made a down payment on a USD 30 million deal for the surveillance software[739].

407. However, one year later, a Russian defence official notified Israel about Estonia's intention to use Pegasus spyware on Russian phone numbers. This information led the Israeli Ministry of Defence to block Estonia from spying on any Russian devices

---

[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.
[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 March 2022.

worldwide, stating that the deal would be harmful to Israeli-Russian relations[740]. The case of Estonia underlines that Pegasus spyware is not just a surveillance weapon, but also serves as political currency in diplomatic relations.

LITHUANIA

408. A Lithuanian company, UAB Communication Technologies, which operates in the area of connection and telecommunication services, is owned by Anatoly Hurgin, a Russian-Israeli citizen, former Israeli military engineer and the co-developer of Pegasus together with NSO[741]. Hurgin also acquired a Maltese golden passport in 2015[742].

BULGARIA

409. In Bulgaria, export controls and export licences for products categorised as dual-use under the EU Dual-Use Regulation are controlled by the Ministry of Economy, and more specifically by the Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction[743]. The current Minister of Economy and Industry is Nikola Stoyanov[744]. The Bulgarian authorities deny having granted export licenses to NSO Group or its subsidiaries[745]. However, former private equity owner of NSO Group Novalpina Capital emphasised that NSO products are being exported from the EU from both Cyprus and Bulgaria[746] [747] [748]. These two claims are contradictory. Furthermore, media publications claim that some of the servers of the network infrastructure over which Pegasus attacks are conducted are located in a Bulgarian data centre owned by a Bulgarian company. This company is owned by NSO Group, Circles Bulgaria and Magnet Bulgaria, which have received export licences from the authorities. From Bulgaria, this subsidiary of NSO Group provides the Cypriot subsidiaries with research and development services and exports network products to governments[749]. Magnet is currently dormant, but Circles is currently still active and has received an export licence that is valid until 25 April 2023[750].

410. In February 2022, the Sofia City Prosecutor's Office launched an investigation to establish whether state services had illegally used Pegasus spyware to target Bulgarian citizens. The investigation is currently ongoing[751]. In January 2022, in the case of

---

[740] The New York Times, 'Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia', 23 March 2022.
[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 February 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.

*Ekimdzhiev and Others* v *Bulgaria*, the ECtHR found that the existing laws in Bulgaria on the secret surveillance and retention and accessing of communications did not meet the quality-of-law requirement of the Convention and asked the government to make the necessary changes to domestic law to end the violation[752].

*I.G. EU institutions*

TARGETING OF THE EUROPEAN COMMISSION

411. On 11 April 2022, Reuters reported that Commissioner for Justice Didier Reynders and at least four Commission staff members had been targeted with Pegasus software in November 2021[753].On 23 November 2021, Apple sent official notifications to the devices of Commissioner Reynders and 'additional Commission staff', informing them that they had been 'targeted by state-sponsored attackers' and their devices might have been compromised[754].

412. Following these revelations, Commissioner Reynders was invited to speak to the PEGA Committee on 30 May 2022 and also responded in writing to its questions. As early as 19 July 2021, following the revelations by Forbidden Stories and Amnesty International, the Commission had set up a 'dedicated team of in-house experts, tasked with an internal investigation', in order 'to verify whether Pegasus had targeted devices of Commission staff and members of the College'[755]. The Commission also deployed a mobile Endpoint Detection and Response (EDR) solution on all corporate phones in September 2021, which helps the Commission's services to identify potentially infected corporate mobile devices.

413. In the course of the investigation, the Commission communicated that, 'neither ... before or after this date [23 November 2021]' had these checks confirmed that Commissioner Reynders's personal or professional devices had been compromised. The Commission's competent services also inspected the devices of the other staff who had received similar notifications from Apple on the same day, but 'none of the inspected devices confirmed Apple's suspicions' either'[756].

414. However, in its letter of 9 September 2022, the Commission acknowledged that in the course of the ongoing investigation into the targeting of the Commission with Pegasus, 'several device checks led to the discovery of indicators of compromise'. The Commission has thus far not elaborated further on the findings of its investigation, either in public or in the PEGA Committee, as 'they would reveal to adversaries the Commission's investigation methods and capabilities, thus seriously jeopardising the institution's security'[757]. Unofficial reports of more than 50 detected infections have not

---

[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.

been confirmed by the Commission.

415. In response to the question by the PEGA Committee as to which actor or actors might be behind these attacks, the Commission responded that 'it is impossible to attribute these indicators to a specific perpetrator with full certainty'. However, the common overarching issue that two of the known targeted Commission officials, Commissioner Reynders and a member of Commissioner Věra Jourová's cabinet[758], deal with is the rule of law. In response to PEGA's question about a possible correlation, the Commission has refused to share further information on the number of departments which may have been compromised, on the professions of the staff affected or any further information that would be of interest to the PEGA Committee's work and could determine the origin of the attack, and it has stated that it does 'not have enough information at its disposal allowing us to draw definitive conclusions about a link between geolocation and a possible device infection attempt via Pegasus'[759].

416. In the light of the above, several problems can be identified. Firstly, the Commission has not demonstrated sufficient awareness and understanding of the enormous political risks involved in being the target of spyware. Any attempted hack – whether successful or not – of the Commission, or one or more of its members, is a very grave political fact that affects the integrity of the democratic decision-making process. In its interactions with the PEGA Committee, the Commission repeatedly explained that the hack of Commissioner Reynders's device with Pegasus software did not succeed. However, as the Commission itself mentioned, 'several device checks [of staff] led to the discovery of indicators of compromise', about which there has been no further communication. This seems to indicate that the Commission is downplaying the gravity of an EU institution being targeted.

417. Secondly, there appears to have been insufficient IT capacity and capability to shield Commissioners and staff against attacks or to monitor and verify their cyber security. Although the Commission has put new measures in place, such as the EDR solution, on all Commission phones, and engages in continuous cooperation with CERT-EU[760], owing to the lack of information PEGA has received from the Commission, it is unclear to what extent the Commission's measures to analyse previous spyware attacks have been successful and to what extent the measures implemented will be sufficient in the future.

418. Thirdly, the Commission did not officially report the notifications or the indicators of compromise to the Belgian police for further investigation, but has only been in contact with the Belgian police on 'technical details' as part of its 'regular cooperation'. The Commission has declared that '[n]otifications of this kind are received multiple times on any given day by the Commission's relevant IT departments' and therefore do not merit being officially reported to the police. According to the Commission, since the Apple notification did not signal a 'definitive infection, but the possibility of an attempt by the malware to target the corresponding device', the Commission did not follow up with law enforcement authorities[761].

[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.
[761] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.

However, in other cases, for example in Spain and France, a criminal investigation has been launched into the use of spyware against government ministers and heads of state. Spyware is used mainly by state actors, citing reasons of national security. The Commission argues that 'some aspects linked to national security fall outside the competences of the Commission'[762], but it fails to explain how Commissioners and Commission staff could plausibly constitute a risk to national security.

419. Fourthly, the fact that the Commission did not provide PEGA with meaningful information, either *in camera*, about the targeting of the Commission, or, more generally, with any basic information related to the investigation, means that Parliament was not able to exercise democratic scrutiny properly. The Commission should reassess what information it can disclose in order to allow for meaningful parliamentary oversight.

TARGETING OF MEMBERS OF THE EUROPEAN COUNCIL, THE COUNCIL AND THE COMMISSION

420. Not only were one current member of the Commission and other Commission staff targeted, but government leaders, ministers and a former Commissioner were also allegedly targeted with spyware from outside and within the Union.

421. French President Macron's telephone number appeared on the Pegasus Project list of potential targets and the Spanish Government confirmed that the phones of Spanish Prime Minister Pedro Sanchez, Minister of Defence Margarita Robles and Minister of the Interior Fernando Grande-Marlaska were infected with Pegasus spyware, allegedly from outside the Union.

422. According to the Greek newspaper Documento, which published an extensive list of people who have allegedly been found to have traces of Predator on their devices[763], Dimitris Avramopoulos, who was a European Commissioner from 2014 to 2019, and several current government ministers, including the Minister of Foreign Affairs and the Minister of Finance, were targeted with spyware. . It is not clear whether the alleged hacking attempts on Avramopoulos happened while he was member of the Commission, nor is it clear who was behind them. However, the long list of targeted people includes many Greek politicians from both the governing party and the opposition.432. These confirmed and alleged infections and hacking attempts demonstrate that it might be possible for current government leaders and ministers, and current or former Commissioners, including their communications with colleagues, to be targeted from outside or within the Union while they are members of the European Council, the Council and the Commission. Therefore, a single infected phone could also seriously compromise information held by the institutions, including information shared during Commission and Council meetings in real time.

*I.H. Third countries*

423. The following section will highlight the extent to which the use of Pegasus or

[762] Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 July 2022.
[763] Documento, edition of 6 November 2022.

equivalent surveillance spyware, directly or indirectly involving entities linked to the EU, contributed to illegal spying on journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors, human rights defenders or other actors in third countries. This includes the extent to which the deployment of spyware has led to human rights violations that are of serious concern as regards the objectives of the EU's common foreign and security policy, and whether the spyware's use was in contravention of the values enshrined in Article 21 TEU and in the Charter, also with due regard to the United Nations Guiding Principles on Business and Human Rights and other rights enshrined in international human rights law.

424. Of the third countries involved with spyware, Israel and Morocco have received particular attention from the PEGA Committee, with a hearing and mission to Israel in July 2022 and a session dedicated to Morocco in February 2023 during a hearing on the geopolitics of spyware. In addition, a hearing in August 2022 was partly dedicated to Rwanda, with remarks from Carine Kanimba, who was a target of Pegasus.

ISRAEL

425. The PEGA Committee visited Israel in July 2022. The main purpose of the trip was to meet with the manufacturer of Pegasus spyware, the Israeli-based company NSO Group. The PEGA delegation learned that NSO Group has sold spyware to 14 EU governments, using export licences issued by the Israeli Government. They discussed abuses of mercenary surveillance tools and their impact on democracy, the rule of law and fundamental rights in the EU. The Committee also met with representatives of the government, the Knesset, experts and civil society. This visit underlined the ineffectiveness of existing safeguards against the abuse of spyware and the need for much tighter European Union regulation of the sale, purchase and use of spyware. The area of cyber intelligence needs to be regulated effectively to prevent the abuse of spyware in future.

426. Israel's geopolitical and security situation has prompted its government and private sector to develop intelligence-gathering tools that would expand the country's cybersecurity capabilities, especially with regard to its defence. Over the years, Israel has become one of the world's leading producers of advanced surveillance technologies and spyware, as it has considerable expertise in developing intelligence-gathering tools. The industry exports its products globally. A study commissioned by the European Parliament and published in 2023 under the title 'Pegasus and the EU's external relations' noted that 'for exporting countries, the spyware industry can be a lucrative source of revenue and a lever for diplomatic influence'[764]. This is also confirmed by news reports, with experts highlighting the usefulness of Pegasus in forging diplomatic relations, e.g. with Gulf states[765].

427. In addition to strategic domestic reasons, Israel has successfully promoted itself as an innovative start-up nation, with firms with the most sophisticated technology in the field, such as NSO, Cellebrite, Candiru, QuaDream and Intellexa. The industry's

[764] '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.
[765] https://www.france24.com/en/livenews/20210719-pegasus-scandal-showsrisk-of-israel-s-spy-tech-diplomacyexperts.

collective sales are estimated to be at least USD 1 billion annually[766], amounting to about 0.6 % of Israel's exports[767]. Israel's defence forces and intelligence agency, particularly its cybersecurity division Unit 8200, have played an essential role in Israel's successful spyware industry and firms enjoy close relations with the entity. According to a 2018 study, 80 % of the 2 300 people who founded Israel's 700 cybersecurity companies were former employees of the Israeli Defence Forces' intelligence units. One of its most prominent figures in the industry is Intellexa owner and founder Tal Dilian (see the section on Intellexa and Tal Dilian)[768].

428. Israeli spyware companies have sold surveillance technology throughout the world, including to EU Member States and authoritarian Gulf countries. According to the newspaper Haaretz, the sale of Pegasus was used as a diplomatic bargaining chip and facilitated the negotiations for establishing formal diplomatic ties with Morocco, Bahrain and, formally, the United Arab Emirates under the Abraham Accords[769]. The sale of spyware to authoritarian regimes has been criticised, especially in the wake of the Pegasus Project. As a result, in December 2021 the Israeli Government tightened export rules for cyber warfare equipment. In the light of Israel's planned judicial overhaul, many Israeli tech companies are reportedly being offered incentives by Greece, Cyprus and Portugal to relocate their businesses to these countries. According to media reports, the three countries are allegedly offering Israeli tech companies tax breaks, while Greece is reportedly providing fast-tracked citizenship[770].

429. According to experts, Israel's readiness to test new surveillance systems on Palestinians in the occupied territories creates incentives for a business model in the surveillance industry, which NSO, too, has benefited from[771]. As a result, countries acquiring 'field-trained' spyware from Israel are contributing to human rights violations in the aforementioned regions. EU Member States, as some of NSO's most prestigious clients, are therefore in direct contradiction of the EU's foreign and security policy agenda regarding the support of human rights and democracy[772].

430. NSO's Pegasus spyware has been used to target Palestinian civil society, including six Palestinian human rights defenders[773]. In the cases of Ubai Al-Aboudi, executive

---

[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.
[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] In line with most of the findings of the Commission's 2021 annual report on the application of the EU Charter of Fundamental Rights, entitled 'Protecting Fundamental Rights in the Digital Age', the EU is required to facilitate the work of human rights defenders online.
[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/.

director of the Bisan Center for Research and Development, and Salah Hammouri, a dual French-Palestinian national, lawyer and field researcher at the Addameer Prisoner Support and Human Rights Association, the use of surveillance spyware appears to have resulted in their administrative detention. The surveillance of all six individuals coincides with the highly controversial designation of six Palestinian human rights organisations as 'terrorist', sparking an international outcry condemning the decision by the Israeli Government. This instance of surveillance of Palestinian human rights defenders is yet more proof of the lack of enforcement of NSO's human rights policy[774], which the company has used to boost its legitimacy and credibility when selling to EU Member States.

431. It should be noted that the Commission has engaged with the Israeli authorities regarding reports of misuse of NSO's Pegasus spyware in violation of human rights. In a letter to the PEGA Committee dated 9 September 2022, the Commission replied that it had addressed concerns of potential misuse with the Israeli export authorities and 'sought indications on any related mitigating measures that competent Israeli export control authorities could consider taking in the future'. At the time of the letter, the Commission had not received any such indications from the competent Israeli export control authorities but intended 'to return to the issue of possible mitigating measures at the next meeting of the EU-Israel Subcommittee on Industry, Trade and Services of the Association Agreement'.

MOROCCO

432. Multiple news reports have documented the alleged widespread use of spyware by Morocco. With a licence for about 100 000 phone numbers, Morocco can be considered one of NSO's biggest Pegasus clients[775]. Morocco has refuted the accusations tied to the Pegasus Project as 'erroneous'. In December 2020, a Citizen Lab report revealed that Morocco is one of the 25 customers of Circles, a subsidiary of NSO Group[776].

433. The revelations also demonstrated that within the country, surveillance with spyware has allegedly been used to hack and subsequently intimidate journalists and activists[777]. In a recent resolution on the surveillance and imprisonment of investigative journalist Omar Radi, the European Parliament condemned the Moroccan Government's sustained judicial harassment against journalists and urged the Moroccan authorities 'to end their surveillance of journalists, including via NSO's Pegasus spyware'[778]. One of the targeted individuals, Ignacio Cembrero, an investigative journalist at the Spanish newspaper El Confidential, appeared before the PEGA Committee on 29 November 2022. He became aware that his phone had been hacked after text messages between him and the Spanish Government were published in a Moroccan newspaper. When a Spanish court requested their cooperation, the Israeli authorities refused to supply further information to aid the case.

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

434. Morocco has also persecuted Moroccan journalists Hicham Mansouri and Aboubakr Jamaim[779], who are in exile in France, as well as supporters of Western Sahara, including Paris-based defence lawyer Joseph Breham and Belgium-based Sahrawi human rights defender El Mahjoub Maliha[780].

435. Morocco has launched several legal proceedings in response to accusations of its involvement in the use of Pegasus in France, Spain, and Germany. In France, the Moroccan authorities filed defamation suits against several media outlets and civil society organisations, including Le Monde, Forbidden Stories, Radio France, Mediapart, L'Humanité and Amnesty International. On 25 March 2022, the Paris Criminal Court dismissed the cases as inadmissible and the Moroccan authorities appealed the decision. In Spain, the Moroccan authorities filed a case against journalist Ignacio Cembrero on the basis of a medieval clause in the Penal Code, accusing him of 'an act of bragging". The case is ongoing and has been denounced as an attempt to deter Cembrero and others from reporting on Morocco's use of the spyware[781].

436. According to a news report, prior to its widespread use of Pegasus, Morocco was also a client of at least three European spyware providers, namely the French companies Amesys and Vupen[782] and the Italian company Hacking Team. According to confidential documents, Morocco was the third largest client of the Italian company and paid more than EUR 3 million over six years to acquire Hacking Team's RCS software for its domestic High Council for National Defence (CSDN) and the Directorate of Territorial Surveillance (DST)[783]. Multiple high-level UN departments and services have been surveilled using the spyware.

437. Morocco has not only acquired spyware in the EU, but has also been supplied with technological and financial support by the European Commission. According to Der Spiegel, Morocco received two spyware systems from the EU to spy on individuals for border control purposes (French-Lebanese MSAB's spyware XRY and US-based Oxygen Forensics spyware Detective)[784]. In addition, the European Union Agency for Law Enforcement Training (CEPOL) was sent to Morocco to conduct in-person training on how to use spyware and to teach the police how to extract information from social media profiles via social hacking[785]. Contrary to Pegasus, the abovementioned spywares can only enter devices physically and do not leave any traces of their use. The report outlines multiple cases in which smartphones were taken away from targets, among them journalists and activists, and returned with hints about their possible infection.

---

[779] Forbidden Stories. https://forbiddenstories.org/journaliste/hicham-mansouri/, https://forbiddenstories.org/journaliste/aboubakr-jamai/.
[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.

Although it is not possible to verify whether spyware has been used properly by third parties, there were no indications that the Commission had verified the proper use of the supplied technologies. Mirroring the situation similar described in a complaint to the EU Ombudsman about funding for surveillance technologies under the EUTFA programme (see the relevant section below), no impact assessment has been conducted by the Commission to map potential misuse of the supplied technologies. The Commission has stated that it is up to the user, Morocco, to deploy the spyware responsibly and in accordance with the contractual agreement (i.e. for the purposes outlined in the agreement only)[786].

OTHER THIRD COUNTRIES

438. Globally, at least 75 countries have purchased and/or used spyware, including repressive regimes[787] . Human rights organisations have documented numerous incidents where spyware has been misused to target politicians, journalists, lawyers, human rights defenders and other civil society activists promoting human rights, women's rights and environmental protection[788] .

EU MEMBER STATES' COMPLICITY, AS NSO GROUP CLIENTS, IN PEGASUS ABUSE IN THIRD COUNTRIES

439. The authorities of 14 non-EU countries are most likely responsible for many cases in which where the targeted people have been identified and the infection was technically proven. The countries in question are El Salvador, Mexico, Thailand, Morocco, India, Rwanda, Saudi Arabia, Bahrain, Jordan, Kazakhstan, Togo, the UAE, Israel and Azerbaijan[789].

440. The Pegasus Project, a collaboration by more than 80 journalists from 17 media outlets, has documented how Pegasus has been used by repressive governments seeking to silence journalists, attack activists and crush dissent. Investigations by the Pegasus Project have shown that family members of Saudi journalist Jamal Khashoggi were targeted with Pegasus spyware before and after his murder in Istanbul on 2 October 2018 by Saudi operatives, despite repeated denials from NSO Group. Amnesty International's Security Lab established that Pegasus spyware was successfully installed on the phone of Khashoggi's fiancée Hatice Cengiz just four days after his murder. His wife Hanan Elatr was also repeatedly targeted with the spyware between September 2017 and April 2018, as was his son, Abdullah, who was selected as a target along with other family members in Saudi Arabia and the UAE[790].

441. In addition, the Pegasus Project has documented that journalists have been frequent targets of Pegasus spyware. In Mexico, journalist Cecilio Pineda's phone was selected

---

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

for targeting just weeks before his killing in 2017. Pegasus has also been used in Azerbaijan, a country where only a few independent media outlets remain. According to the investigation, more than 40 Azerbaijani journalists were selected as potential targets. Amnesty International's Security Lab found that the phone of Sevinc Vaqifqizi, a freelance journalist for independent media outlet Meydan TV, was infected over a two-year period ending in May 2021. In India, at least 40 journalists from nearly every major media outlet in the country were selected as potential targets between 2017 and 2021. Forensic tests revealed that the phones of Siddharth Varadarajan and MK Venu, co-founders of independent online outlet The Wire, were infected with Pegasus spyware as recently as June 2021[791].

442. Human rights defenders continue to be targeted frequently, including by the authorities of the following countries: Mexico, El Salvador, Morocco, Rwanda, Israel, Jordan, Saudi Arabia, Bahrain, the United Arab Emirates, India, Kazakhstan, Indonesia and Belarus[792]. In 2021, Frontline Defenders published a report documenting the targeted surveillance of human rights defenders in countries including India. In June 2018, 16 human rights defenders were jailed under Indian anti-terror legislation in what is known as the Bhima Koregaon case, which relates to the violence that took place in Bhima Koregaon. One of the human rights defenders, 84-year-old Jesuit priest Stan Swamy, died in custody in July 2021[793]. A digital forensics investigation found that 'evidence' relied on by the prosecution against the group had been planted, using Pegasus spyware, on devices belonging to the human rights defenders Rona Wilson and Surendra Gadling, and that there was no evidence that the human rights defenders had interacted[794].

### *II. The spyware industry*

443. The European Union is an attractive place for the trade in surveillance technologies and services, including spyware tools. On the one hand, the Member State governments are potential customers. On the other hand, the idea of being 'EU-regulated' serves as a benchmark, which is useful for the global market. The EU internal market offers freedom of movement and beneficial national tax regimes. Procurement rules can be avoided with reference to national security, and governments may use proxies or middlemen, so that the purchase of spyware by public authorities is very hard to detect and prove. The EU has strict export rules, but recently, there has been a trend of the Member States circumventing these and seeking to get a competitive advantage with improper national implementation. Furthermore, enforcement by the European Commission has often been inadequate . Indeed, each time the regime for export licenses was tightened in Israel, several companies moved their export departments to

[791] Amnesty International, 'Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally', 19 July 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 December 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 December 2021, https://thewire.in/rights/rona-wilsonpegasus-iphone-arsenal.

Europe, in particular Cyprus[795] [796]. Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.

444. Further, as head of Amnesty Tech Claudio Guarnieri testified before the PEGA Committee, it was European companies like the German FinFisher and the Italian Hacking Team that pioneered the mercenary spyware industry. The first reports on the roles of these companies in monitoring journalists and crushing dissent came out over ten years ago when, with the advent of the protest movements known as the Arab Spring, contracts with these companies started emerging from offices of the secret police[797].

445. The spyware industry has an obfuscating structure, built on a complex web of persons, locations, connections, ownership structures, letterbox companies, ever-changing corporate names, money flows, government proxies and middlemen, tycoons and governments.

446. In many cases, the nickname 'mercenary spyware' seems to be accurate. As the number of persons illegally targeted demonstrates, many companies fall behind with regard to ethical standards, often selling to dictatorships and wealthy non-state actors and continuing to do so even after the Pegasus Project revelations. In 2021 Cellebrite announced it would stop selling to the Russian Government when it became known that its spyware had been used on anti-Putin activists. However, in October 2022 there were signs that Cellebrite was still being used by the Russian authorities[798]. It is a lucrative and ambiguous market. Still, many spyware companies are able to sell their products to democratic governments in the US and the EU, which grants a veneer of respectability. Nonetheless, despite claims that the use of spyware is entirely legitimate and necessary, governments are hesitant when it comes to admitting they possess spyware. They sometimes resort to the use of proxies, middlemen or brokers for the purchase of spyware, so as to leave no traces. The big annual event for the industry is the 'ISS World' fair, also dubbed 'The Wiretappers' Ball'. The home of the annual European edition is Prague. There is considerable overlap between the exhibitors at ISS World and the exhibitors at arms industry fairs.

447. Besides the 'official channels', there is also a black market for these products. Although many vendors claim they only sell to governments, it appears they also try to do business with non-state actors. It is very difficult to find watertight evidence, as this trade leaves few traces. Greek newspaper Documento claims to have evidence that the software is being sold on the black market – for up to USD 50 million – not only to governments and counter-terrorism agencies, but also to private individuals[799]. Another Greek newspaper, To Vima, reported that Predator was sold to 34 customers from Greece[800]. Leaked documents show that a pirated version of the product that was

[795] Makarios Drousiotis, 'State Mafia', 2022, Chapter 6.
[796] Haaretz. 'Cyprus, Cyberspies and the Dark Side of Israeli Intel'.
[797] PEGA hearing of 30 August 2022 on the impact of spyware on EU citizens, 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.
[799] Documento, 'Documento's "Predator" revelations on Euractiv – Europol's intervention calls for Dutch MEP'.
[800] To Vima, Interceptions 'Spy software has 34 customers'.

officially sold only to governments was available at a price of USD 8 million, an amount that included training the agents who will use the program, 24-hour technical support and monitoring of the target's social media accounts[801].

448. The industry offers a wide range of surveillance and intelligence products and services, not just spyware as a single product. Spyware is just one tool in the toolkit of hack-for-hire firms.

*Vulnerabilities*

449. Without software vulnerabilities, it would be impossible to install and deploy spyware. Therefore in order to regulate the use of spyware, the discovery, sharing and exploitation of vulnerabilities have to be regulated as well[802]. Despite the strengthening of the defence of digital systems required and encouraged by the NIS2 Directive and the proposal for the Cyber Resilience Act, it is nearly impossible to develop systems without vulnerabilities.

450. Vulnerabilities therefore need to be disclosed and fixed as soon as possible. However, current EU law encourages the opposite of disclosure. Under the Cybercrime Directive and the Copyright Directive, information security researchers may face civil and criminal liability when doing research into vulnerabilities and sharing their results. Moreover, it is not obligatory for researchers to share any findings on vulnerabilities. Researchers could therefore opt to sell their knowledge of a vulnerability to a private broker in return for high remuneration.

451. This practice has generated a lively and lucrative trade in vulnerabilities. However, it is not just brokers in zero-days vulnerabilities who are looking for vulnerabilities: security and law enforcement authorities stockpile vulnerabilities as well, some found by their own experts, some acquired from brokers. If vulnerabilities go unreported, they are not patched, leaving IT systems weakened and the users unprotected. This allows the use of spyware to continue.

*Telecom networks*

452. Telecom providers play a significant role in the process of spying, both legal and illegal. We are living in a modern era of AI, big data and quantum computing, but at the same time we are using and strongly relying on an international telecommunication protocol called Signalling System No 7 (SS7). This protocol was developed in 1975 and is still used today. This system controls how telephone calls are routed and billed and enables advanced calling features and Short Message Service (SMS)[803]. Via the SS7 network, it is possible to intercept phone calls and SMS messages, identify geolocations and infect

[801] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/.
[802] Ot van Daalen, intervention in PEGA Committee, 27 October 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.
[803] https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7 was first adopted as, up to and including 5G.

a target with spyware, such as Pegasus or Predator[804].

453. The risk of abuse by the telecom providers of access to these networks is high. There are several documented cases of misuse, where access points (global titles) were leased to companies that monitored and intercepted targets' communications using man-in-the-middle attacks. They also harvested geolocation data and metadata for their own economic purposes. A global title is an address used for routing messages within SS7. It can be compared to an IP address, in that the global title is an address within the telecommunications system[805]. According to a whistleblower, this is why NSO was so interested in access to the SS7 network in the US that it tried to buy access from their company[806]. Telecom providers deliberately keep industry standards low in order to provide easier access to local state enforcement agencies.

*The NSO Group*

454. Pegasus spyware is produced by the NSO Group. The NSO Group was founded in 2010 by Shalev Hulio, Omri Lavie and Niv Karmi, developing technology to help licensed government agencies and law-enforcement agencies to detect and prevent terrorism and crime[807]. Pegasus spyware is the best known product of the NSO Group. It was brought onto the global market in 2011[808] [809].

455. Since its launch in 2010, the NSO Group has had a corporate presence in Israel, the UK, Luxembourg, the Cayman Islands, Cyprus, the US, the Netherlands, Bulgaria and the British Virgin Islands. A lot of information regarding the roles of the different corporate entities is still lacking and some of these companies have already been liquidated. However, the NSO Group stated in its 2021 transparency and responsibility report that Bulgaria and Cyprus are both export hubs[810]. According to Amnesty International, the Dutch entities (liquidated on 22 December 2016) functioned in the sector of financial holdings, while Luxembourg-based Q Cyber Technologies was active as a commercial distributor responsible for issuing invoices, signing contracts and receiving payments from customers. In addition, US-registered Westbridge Technologies may have facilitated the company's US sales[811].

456. NSO reportedly had revenues of USD 243 million in 2020[812]. However, following the revelations by the Pegasus Project, the company faced several difficulties. Lawsuits filed by Apple[813] and Meta[814] against the company, the blacklisting of NSO by the US Commerce department, the tightening of the Israeli export regime, critical inquiries in several countries, and internal frictions within the private equity fund behind the NSO

[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.
[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 February 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'.

Group have led to a severe decline in profit. At one point the NSO Group's debt reportedly even reached 6.5 times its normal annual revenues[815].

457. The PEGA Committee had two meetings with the NSO Group, of which one took place in Brussels and one in Israel. Pegasus spyware was initially sold to 22end-users in 14 EU Member States, using marketing and export licences issued by Israel. Contracts with end-users in two Member States were subsequently terminated[816]. It has not been confirmed which Member States are included in the list of 14, nor which two countries were removed. However, it could be assumed the two are Poland and Hungary.

CORPORATE STRUCTURE, TRANSPARENCY AND DUE DILIGENCE

458. On 25 January 2010, the NSO Group launched its first company in Israel. This company was registered under the name 'NSO Group Technologies Limited'. The NSO Group is both the name of the first registered company and the umbrella term for the various companies established in other jurisdictions. This first established company is the owner of the NSO Group trademark[817].

459. In March 2014, private equity fund Francisco Partners obtained a 70 % stake in the NSO Group. Under Francisco Partners, the company expanded its entities to different jurisdictions, including Cyprus, Bulgaria, the US, the Netherlands and Luxembourg. During the Francisco Partners years (2014 to 2019), the fund systematically reviewed the sale of the NSO Group's products through the Business Ethics Committee (BEC). According to Francisco Partners, the BEC denied tens of millions of dollars' worth of sales that would have otherwise be approved of under legal requirements[818].

460. Francisco Partners sold its entire ownership interest, including that in the subsidiaries, to Novalpina Capital on 14 February 2019. With this management buyout, the governance standards changed and the BEC was replaced by the Governance, Risk and Compliance Committee (GRCC) for the review of the human rights records of potential customers[819].

461. In line with the End Use/User Certificate, after the tightening of the Israeli export regime, the NSO Group introduced a human rights policy and a human rights due diligence procedure. As described in the NSO Group's 2021 transparency and responsibility report, the NSO Group requires that all customer agreements include human rights compliance clauses and clauses outlining the suspension or termination of the use of the NSO Group's products in the event of human-rights-related misuse. In a written submission to PEGA, the NSO Group confirmed that it has terminated contracts with EU Member States[820] that supposedly breached the human rights clauses. The NSO Group has not clarified if it examined the audit logs and whether the customers in question had consented to an examination. It is therefore not known if any evidence of the abuse still exists, if NSO has any way of preserving that evidence or if the Israeli

[815] Bloomberg, 'Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop'.
[816] Answers provided by NSO Group to PEGA secretariat following hearing, 20 July 2022.
[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] PEGA Committee hearing with NSO, 21 June 2022.
[820] PEGA Committee hearing with NSO, 21 June 2022.

authorities have any evidence.

462. According to Amnesty International, the NSO Group's transparency report lacks a proper remediation policy for persons targeted by unlawful surveillance, and there is no information on the ongoing lawsuits against the NSO Group[821]. NSO spyware continues to be detected on the devices of journalists and critics of authoritarian regimes, contrary to NSO's human rights policy and human rights due diligence procedure[822].

EXPORT CONTROLS

463. Since Pegasus spyware is classed as a dual-use technology, it needs to receive an export licence. The NSO Group companies obtain their export licences in Israel, Bulgaria and Cyprus[823].The NSO Group itself has confirmed this, but denies that Pegasus spyware is exported from Cyprus and Bulgaria[824]. The Cypriot and Bulgarian governments have denied granting any export permits to NSO companies in general. Other sources have challenged this, stating that NSO subsidiaries often hide behind a different name in national business registers. However, one of NSO's subsidiaries in Cyprus, operating under the name 'Circles' closed its offices in 2020[825]. Licences are also granted by the Israeli authorities[826]. Israel is not part of the Wassenaar Arrangement but states that it has incorporated some of its elements into the Israeli national Defence Export Control Law No 5766-2007[827]. The Ministry of Defence's Defence Export Control Agency is responsible for issuing marketing and export licences[828]. Following the Pegasus Project revelations and the blacklisting of NSO, the list of eligible countries has been reduced from 102 to 37, all of which need to sign an End Use/User Certificate[829]. Under the due diligence procedure, Israel automatically considers all EU Member States compliant with EU standards, so it will not conduct additional assessments for individual countries. However, the decision to terminate the contracts with two EU Member States seems to indicate that the EU is no longer considered a single entity for the purpose of due diligence.

UNETHICAL BEHAVIOUR TRIGGERING LAWSUITS, BLACKLISTING AND INVESTOR CONFLICTS

464. In July 2021, a conflict between the three co-founders of Novalpina Capital started to affect the NSO Group's business, eventually leading investors to the decision to strip the private equity firm of its control[830]. On 27 August 2021, US consultancy firm Berkeley Research Group (BRG) took over the private equity fund and launched critical investigations into the lawfulness of the NSO Group's activities and its compliance with the US blacklisting. BRG's May 2022 inquiries were obstructed by the NSO Group's

[821] Amnesty International, 'NSO Group's new transparency report is "another missed opportunity"', press release, 1 July 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', p. 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] European Parliamentary Research Service, '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] European Parliamentary Research Service, 'Europe's PegasusGate – countering spyware abuse'.
[830] Financial Times, 'Private equity owner of spyware group NSO stripped of control of €1bn fund'.

management team[831]. A BRG executive stated that cooperation with the NSO Group had become 'virtually non-existent' due to the NSO Group's pressure for continued sales to countries with controversial human rights records[832]. On 25 April 2022, two of Novalpina's former general partners filed a lawsuit at a Luxembourg court against BRG, demanding that Novalpina Capital be reinstated as a general partner and that all decisions made by BRG be suspended[833]. The Luxembourg court dismissed these demands, and BRG remains in charge of the fund controlling the NSO Group[834].

465. In addition to ownership fall-outs, on 3 November 2021 the US Commerce Department placed the NSO Group on a blacklist due to the incompatibility of NSO's activities with US foreign policy and national security concerns. The US administration prohibits the export of technology to the NSO Group and its subsidiaries, *de facto* meaning that no American company can work with the NSO Group[835].

466. In response to the US blacklisting, Credit Suisse, one of the creditors of the NSO Group, allegedly pushed the company to continue its sales of Pegasus spyware to new customers. In a letter to BRG sent by Willkie Farr & Gallagher, several creditors stated that they were concerned that BRG was preventing the NSO Group 'from pursuing and obtaining new customers'. Although not explicitly stated in the letter, two experts on the matter stated that one of the creditors was Credit Suisse. BRG responded to the lenders that it was deeply concerned that they were pressing for the NSO Group to make sales[836].

467. A few days after the US blacklisted NSO, the United States Court of Appeals confirmed that Meta's lawsuit against NSO could proceed. Immediately afterwards, Apple lodged a complaint against NSO at the federal court[837]. In June 2022, the United States District Court rejected the NSO Group's claim to immunity in the Apple lawsuit[838]. At time of writing, the Apple lawsuit against the NSO Group is still pending.

468. Despite NSO's blacklisting by the US, the Biden administration allegedly appointed a former NSO advisor, Jeremy Bash, to an intelligence advisory board in October 2022. Under the auspices of Beacon Global Strategies, Bash was reportedly hired to advise the NSO Group through Francisco Partners. According to the Guardian, he was one of the eight members on NSO's business ethics committee, which allegedly gave him a vote on proposed NSO sales. Beacon Global Strategies terminated its work with NSO after the group pursued sales to Saudi Arabia[839].

469. The NSO Group has similarly suffered from staff departures. Since the murder of Jamal Khashoggi and amid growing concerns about the role of Pegasus therein, many employees have left the NSO Group. That same month, co-founder Shalev Hulio

---

[831] Financial Times, 'NSO Group keeping owners 'in the dark", manager says'.
[832] The New Yorker, 'How democracies spy on their citizens'.
[833] Letter to Mr Jeroen Lenaers and his Vice-Chairs.
[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/.
[839] The Guardian, 'Biden intelligence advisor previously vetted deals for Israeli NSO Group'.

stepped down as CEO of the NSO Group and was replaced by Yaron Shohat[840]. The NSO Group changed policy and now focuses only on NATO members[841]. In March 2023, it was reported that NSO shares had been transferred to co-founder Omri Lavie's investment firm Dufresne Holding[842].

470. The pressure on the NSO Group has created demand for other spyware companies. The Financial Times reported on 31 March 2023 that the Indian Government was allegedly searching for an opportunity to purchase alternative commercial spyware with similar functionalities to the now-controversial Pegasus spyware, and that it was also considering also Intellexa's Predator spyware[843].

471. In October 2022, Shalev Hulio and former Chancellor of Austria Sebastian Kurz launched a new cybersecurity firm called Dream Security. Kurz stepped down as chancellor after a corruption scandal in October 2021 and started working for Peter Thiel's investment firm two months later. The company will produce solutions in the field of cyber incidents, centring on artificial intelligence, and will focus its sales on the European market[844]. The cooperation between Kurz and Hulio constitutes an indirect but alarming connection between the spyware industry and Peter Thiel and his firm Palantir.

472. Dream Security raised USD 20 million from several investors, such as Adi Shalev, who was also involved in investments in NSO. Other investors include Yevgeny Dibrov[845], who represents 'the New Russian voice' in what he calls 'the Russian-Israeli tech ecosystem'[846]. This shows that, despite the turbulence and economic challenges encountered by the NSO Group, the same names keep launching new spyware companies within and beyond the EU.

*BLACK CUBE*

473. Black Cube is an Israeli private intelligence agency composed of former employees of the Israeli military and Israeli intelligence services[847]. Its own company website describes it as a 'creative intelligence service' finding 'tailored solutions to complex business and litigation challenges'[848]. Black Cube has been involved in a number of public hacking controversies in countries including the US and Romania[849]. More specifically, the heads of Black Cube admitted to spying on the former chief prosecutor of Romania's National Anti-Corruption Directorate, Laura Kövesi[850]. Kvesi is currently

---

[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'.
[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 October 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'.

the first European Chief Prosecutor, i.e. the head of the European Public Prosecutor's Office (EPPO). Former Romanian secret agent Daniel Dragomir was allegedly the person who commissioned Black Cube for the job[851].

474. Critically, it has also been uncovered that Black Cube is linked with the NSO Group and Pegasus spyware. After much public pressure regarding NSO hiring Black Cube to target their opponents, former NSO CEO Shalev Hulio admitted to hiring Black Cube in at least one situation in Cyprus.

475. Black Cube was involved in Hungary during the 2018 elections, when it spied on various NGOs and persons who had any connection to George Soros and reported back to Viktor Orbán for him to spin their activities in a smear campaign[852]. The information obtained from the surveillance of these individuals and NGOs appeared not only in the Hungarian state-controlled media, but also in the Jerusalem Post[853].

*INTELLEXA ALLIANCE*

476. Intellexa was set up in 2019 in Cyprus by Tal Dilian. Dilian held different leadership positions in the Israeli Defence Force before he started a career as an 'intelligence expert, community builder and serial entrepreneur'[854]. On its website, Intellexa Alliance is described as an EU-based and -regulated company whose purpose is to develop and integrate technologies to empower intelligence agencies. The surveillance vendors that are part of the Intellexa Alliance marketing label include Cytrox, WiSpear (later renamed Passitora Ltd), Nexa Technologies (run by former Amesys managers) and Poltrex.

477. All these vendors facilitate different systems. Whereas Cytrox is skilled in the extraction of data from mobile phones, Nexa Technologies offers exploitation of global mobile communication systems. WiSpear can also extract data from Wi-Fi networks. The different vendors under Dilian's alliance thus provide a broad assortment of software and services, which Intellexa can offer, individually or combined, to its clients within and outside the EU[855].

478. Intellexa Alliance's parent company, Thalestris Limited, has different subsidiaries with a corporate presence in Ireland, Greece, the British Virgin Islands, Switzerland and Cyprus. Sara Aleksandra Hamou, reportedly Tal Dilian's second ex-wife, has been the director of Thalestris Limited and the managing director of a subsidiary based in Greece[856]. Hamou, who was born in Poland, holds a Cypriot passport issued by the

---

[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 July 2018.
[853] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 July 2018.
[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, Annual Report and Consolidated Financial Statements for the period from 28 November 2019 to 31 December 2020.

Embassy of Poland in Cyprus[857].

*WISPEAR AND CYTROX*

479. In 2013, Tal Dilian started a Cypriot-registered company under the name of Aveledo Ltd, later to be known as Ws WiSpear Systems Ltd, then Passitora Ltd[858]. Based in Limassol, Cyprus, Wispear mostly sells equipment and software to locate and track individuals through their mobile phones. In an interview with Forbes magazine, Dilian explained the capabilities of WiSpear software by demonstrating his USD 9 million black van that could hack devices within a range of 500 metres. WiSpear also owns equipment capable of intercepting data from Wi-Fi networks[859]. Public scandals relating to these products triggered the move of Intellexa's main business activities from Cyprus to Greece.

480. In 2017, Cytrox Holdings Zrt. was founded in North Macedonia by Ivo Malinkovski. However, Cytrox actually originated in Tel Aviv, and Malinkovski was just a front. After the Pegasus Project revelations, Malinkovski tried to erase all traces connecting him to Cytrox.

481. Cytrox was the developer of Predator spyware. In contrast to Pegasus spyware, Predator requires the target to click on a link to install the software[860]. When Cytrox was on the verge of bankruptcy, Tal Dilian rescued it, with the acquisition costing under USD 5 million[861]. Cytrox was subsequently merged with Dilian's WiSpear[862]. This acquisition added Predator spyware to the arsenal of Intellexa technologies. As reported by Lighthouse Reports, in collaboration with Haaretz and Inside Story, Intellexa secretly and illegally delivered Predator spyware to the Sudanese Rapid Support Force militia using a Cessna private jet[863].

482. According to Citizen Lab, two Cytrox companies have been registered in Israel (Cytrox EMEA Ltd. and Cytrox Software Ltd) and one in Hungary as (Cytrox Holdings Zrt.)[864]. All of the shares in Cytrox Holdings Zrt. and Cytrox EMEA Ltd – later renamed Balinese Ltd – were transferred to Aliada Group Inc., which is registered in the British Virgin Islands. Aliada Group is also the owner of WiSpear. The main shareholders in Aliada Group are Dilian himself, Oz Liv, Meir Shamir and Avi Rubinstein. In December 2020, Rubinstein lodged a complaint against his fellow Aliada Group shareholders for the illegal dilution of his shares. According to the lawsuit, the relocation of shares to the British Virgin Islands and later to Ireland circumvented Israeli and foreign export control laws[865].

483. On 16 December 2021, Citizen Lab released a report stating that likely Predator

---

[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'.
[860] European Parliamentary Research Service, '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'.

customers had been found in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia and Serbia[866].

*AMESYS AND NEXA TECHNOLOGIES*

484. Amesys and Nexa Technologies are also part of Intellexa Alliance and are not free from controversy, as described in the section on France.

*POLTREX*

485. Poltrex was launched in October 2018 and its sole shareholder was Intellexa Ltd, registered in the British Virgin Islands. Israeli Shahak Avni – the founder of Cypriot firm NCIS Intelligence Services Ltd[867] and an associate of Tal Dilian – was registered as the director of Poltrex in September 2019. In October 2019, both Avni and Dilian became co-directors and Poltrex's name was changed to Alchemycorp Ltd. Even though the company had been renamed, its offices were still in the Novel Tower, the same location as WiSpear's offices[868].

486. When the investigations surrounding Dilian's spyware van were under way, the ownership of Alchemycorp Ltd was transferred to Yaron Levgoren, an employee of Cytrox Holdings[869]. According to Levgoren's LinkedIn profile, he currently represents the Intellexa company Apollo Technologies, based in Greece[870].

*VERINT/COGNYTE*

487. Verint is an Israeli-American cyber company that has many subsidiaries all over the world. In Europe alone, Verint is registered in Bulgaria, the Netherlands, Cyprus, Germany and France (as at 2021). Verint also had subsidiaries operating under the name Cognyte. These subsidiaries have been operating independently since 2021, when Verint completed the spin-off of its intelligence and cyber activities to Cognyte[871]. Cognyte's European subsidiaries are registered in Cyprus (UTX Technologies), Bulgaria (Cognyte Bulgaria EOOD), the Netherlands (Cognyte Netherlands B.V.), Germany (Syborg GmbH, Syborg Grundbesitz GmbH and Syborg Informationsysteme b.h. OHG) and Romania (Cognyte Romania S.R.L.)[872].

488. Verint has sold surveillance tools to several repressive governments, including in Azerbaijan, Indonesia and South Sudan. In the latter case, the South Sudanese National Security Service (NSS) used Verint's interception equipment against human rights activists and journalists between March 2015 and February 2017. According to an Amnesty International inquiry, local mobile operator Vivacell Network of the World

---

[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/.
[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.

enabled the NSS to listen in on all telecommunications in the country[873]. Verint did not respond to questions from Amnesty, but did publish a statement outlining how Verint's independently functioning unit Cognyte is in fact the defence unit whereas Verint solely deals with customer engagement. Verint claims that the division with Cognyte had been in place for many years before the official spin-off in 2021, thus distancing itself from the alleged export of surveillance equipment to countries with poor human rights records[874].

489. Cognyte also has a history of exports to countries with poor human rights records. A 2021 Meta inquiry identified customers in Israel, Serbia, Colombia, Kenya, Morocco, Mexico, Jordan, Thailand and Indonesia[875]. Cognyte subsidiary UTX Technologies, registered in Cyprus, reportedly also received licences for the export of monitoring software to Mexico, the United Arab Emirates, Nigeria, Israel, Peru, Colombia, Brazil, South Korea and Thailand between September 2014 and March 2015[876]. Four of these countries were also identified as Cognyte customers in the 2021 Meta report. In addition, UTX Technologies secured an agreement with Bangladesh for a Web Intelligence System for USD 2 million in 2019 and for a cellular tracking system for USD 500 000 in 2021[877].

490. On 15 January 2023, media reported that Israel's Cognyte Software Ltd had won a tender for the sale of its interception spyware to Myanmar one month prior to the February 2021 military coup. The purchase of Cognyte's spyware by Myanmar officially took place on 30 December 2020[878].

491. As well as exporting to third countries, Cognyte has facilitated the transport of tracking equipment to Member States. Through Cyprus-registered UTX Technologies, Gi2 technology was shipped to another Cognyte subsidiary in Germany, Syborg Informationsysteme[879]. This Gi2 technology was reportedly also sent to a Verint subsidiary in Poland 'for demonstration purposes'. Gi2 technology has the ability to gain access to a particular device and can even impersonate the owner and send false messages through this same device[880]. These shipments took place between 2013 and 2014. At that time, Verint and Cognyte were still part of the same company structure.

492. UTX Technologies also sold monitoring systems in 2013 to a French export company namedf COFREXPORT[881]. This company has ceased operations and is closed at time of writing.

493. Like many other spyware vendors, Cognyte has a highly complex company structure due to name changes, divisions and spin-offs over time. However, the Cognyte subsidiaries show that EU Member States are not only used as bases from which to

[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'.
[875] Meta, Threat Report on the Surveillance-for-Hire Industry.
[876] Philenews, 'Cyprus is a pioneer in software exports' (documents).
[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' (documents).
[879] https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex81.htm.
[880] Philenews, 'Cyprus is a pioneer in software exports' (documents).
[881] Philenews, 'Cyprus is a pioneer in software exports' (documents).

export surveillance equipment, but also as footholds for selling and shipping surveillance equipment within Europe. Israeli spyware companies thus benefit from the EU's internal market, facilitating the transport of their equipment both to their own subsidiaries and to new companies registered in EU Member States.

*QUADREAM*

494. QuaDream is an Israeli company that was founded by a former senior official from Israel's military intelligence, Ilan Dabelstein, and former NSO employees Guy Geva and Nimrod Rinsky. The company is best known for its spyware product Reign, which allegedly makes use of zero-click exploits and includes a self-destruct feature that erases all traces of infection. This type of spyware has different functionalities, such as recording audio, tracking locations, searching for files, and taking pictures through both cameras.[882]

495. According to Citizen Lab and a Microsoft Threat Intelligence analysis, QuaDream systems operate from Bulgaria, the Czech Republic, Hungary, Romania, Ghana, Israel, Mexico, Singapore, the United Arab Emirates and Uzbekistan. In addition, the findings identified at least five civil society targets are located in North America, Central Asia, South-East Asia, Europe and the Middle East.[883]

496. In 2017, a company was registered in Cyprus under the name of InReach. This company was founded solely for the promotion of QuaDream products, like Reign, outside of Israel. Reportedly, QuaDream used InReach to sell its products to customers in order to circumvent Israeli export controls. Many of the key employees of both companies have worked for the NSO Group, Verint and UT-X Technologies.[884]

497. Following Citizen Lab's reporting and the Microsoft Threat Intelligence analysis, it was announced on 16 April 2023 that QuaDream had halted its operations in Israel. According to Haaretz, the company had been struggling with declining sales and employee departures in the preceding months[885].

*CANDIRU*

498. Candiru is another Israeli-registered firm that produces spyware products. The company was founded in 2014 by Ya'acov Weitzman and Eran Shorer. Both founders have a

---

[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.

history in the IDF Military Intelligence Unit 8200 and both were former employees of the NSO Group[886]. Former NSO Group investor Isaac Zack became Candiru's largest shareholder. The company sells spyware for hacking computers and servers[887]. Information disclosed about a project proposal highlights that Candiru sells its equipment on the basis of the number of simultaneous infections, i.e. the number of devices that can be targeted with the spyware at any one time. For example, for USD 16 million, a customer receives an unlimited number of spyware attempts, but can only target 10 devices simultaneously. A customer can purchase the capacity to target 15 additional devices for an extra USD 1.5 million[888].

499. According to a TheMarker inquiry, Candiru now also offers spyware for breaking into mobile devices[889]. It only sells its spyware to governments and has clientele in Europe, the former Soviet Union, the Persian Gulf, Asia and Latin America[890]. The section on Spain mentions that 65 people had been targeted with spyware: of these, four were targeted with Candiru and at least two were targeted with both Candiru and Pegasus[891].

500. As with other spyware vendors, corporate obfuscation lies at the heart of this company, which has undergone several name changes in recent years. The company changed its name to DF Associates Ltd in 2017, Grindavik Solutions Ltd in 2018, Taveta Ltd in 2019 and, most recently, to Saito Tech Ltd in 2020[892]. For sake of clarity, this report refers to the company as Candiru.

501. Just like the NSO Group, Candiru was placed on the US blacklist by the US Commerce Department in November 2021. It is speculated that the reason for Candiru's blacklisting is the fact that NSO Group CEO Shalev Hulio was allegedly a secret partner in Candiru and introduced the company to important middlemen in the intelligence world. Reportedly, Hulio would even argue that Candiru's product is actually a repackaging of Pegasus[893]. On 1 July -2022, security researchers identified a novel Chrome zero-day exploit that was used by Candiru to target individuals in Lebanon, Palestine, Yemen and Turkey[894]. The exploit was addressed by Google and has since also been patched by Microsoft and Apple[895].

*TYKELAB AND RCS LAB*

502. In August 2022, Lighthouse Reports reported that Tykelab, a company based in Rome and belonging to the RCS lab, hadsbeen using dozens of phone networks, often on

[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'.
[895] The HackerNews, 'Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists'.

islands in the South Pacific, to send tens of thousands of secret 'tracking packets' around the world, targeting people in countries including Italy itself, Greece, North Macedonia, Portugal, Libya, Costa Rica, Nicaragua, Pakistan, Malaysia, Iraq and Mali. Tykelab exploits vulnerabilities in global phone networks, which enable third parties to see phone users' locations and potentially intercept their calls without any record of compromise being left on the devices[896]. In just two days in June 2022, the company probed networks in almost every country in the world[897]. On its website, Tykelab states that it 'combines twenty years of experience in the design, implementation and maintenance of Core Network Telco solutions [with] a strong expertise in delivering [m]anaged [s]ervices, [c]ustomer-based [s]ystem [i]ntegration and [m]obile [a]pp developments.'[898].

503. The Lighthouse Reports investigation also highlighted the role of the telecom industry, given that the leasing of phone network access points or 'global titles' allows this abuse to continue. According to GSM Association, the industry organisation representing mobile network operators worldwide, phone operators cannot always identify the source and purpose of the traffic that flows through their networks, which makes it difficult to halt these practices[899].

504. Tykelab is part of RCS Lab, an Italian company known for its interception activities in Italy and abroad. This was brought to light by an announcement by a third company, Cy4Gate, which acquired RCS Lab. RCS Lab has offshoots in France, Germany and Spain[900], as well as another concealed subsidiary, Azienda Informatica Italiana, which builds interception software for Android and iPhone devices[901].

*HERMIT SPYWARE*

505. RCS Lab developed Hermit, a spyware that can be used to remotely activate the targeted phone's microphone, record calls and access messages, call logs, contact lists and photos[902]. In June 2022, Google's Threat Analysis Group revealed that government-backed actors using RCS Lab's spyware worked with the target's internet service provider to disable the target's mobile data connectivity. Once this was disabled, the attacker would send a malicious link via SMS asking the target to install an application to recover their data connectivity. Google believes that this is why most of the applications masqueraded as mobile carrier applications. When the involvement of an internet service provider is not possible, applications are disguised as messaging applications. Persons targeted with RCS Lab's spyware were located in Italy and Kazakhstan[903], and the spyware was also found in Romania[904].

506. A threat intelligence researcher for cybersecurity firm Lookout, Justin Albrecht, said

---

[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/.
[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/.

that although Hermit's installation method was less sophisticated than the method used by Pegasus, its capabilities were similar. Hermit needs a phone user to click on an infected link for it to compromise a device[905].

507. According to RCS Lab, 'any sales or implementation of products is performed only after receiving an official authorisation from the competent national authorities. The products supplied to customers are installed at their facilities, and RCS Lab personnel are not permitted under any circumstances to carry out operational activities in support of the customer or to have access to the processed data. Due to binding confidentiality agreements, RCS Lab cannot disclose any details about its customers. The Cy4gate Group, of which RCS Lab is a member, adheres to the UN Global Compact and therefore condemns all forms of human rights violations. RCS Lab's products are provided with a clear, specific, and exclusive purpose: to support law enforcement agencies in the prevention and suppression of heinous crimes'[906]. However, it is not possible to verify whether Cy4gate Group, including RCS Lab, adheres to its own declared standards.

508. According to a Lighthouse Reports investigation published in August 2022, Tykelab's surveillance tool Hermit was used to target individuals around the world, including in Libya, Nicaragua, Malaysia, Costa Rica, Iraq, Mali, Greece and Portugal, as well as in Italy itself[907].

*DECISION SUPPORTING INFORMATION RESEARCH AND FORENSIC (DSIRF)*

509. A company that has recently become the subject of criminal proceedings by the Austrian Ministry of Justice is DSIRF GmbH (LLC)[908]. Founded in 2016, DSIRF is an Austrian company based in Vienna, with a parent company in Liechtenstein. It claims to provide 'mission-tailored services in the fields of information research, forensics as well as data-driven intelligence to multinational corporations in the technology, retail, energy and financial sectors.'[909]. DSIRF evidently sells to non-state actors.

510. DSIRF developed spyware called Subzero/KNOTWEED, which can be deployed using zero-day vulnerabilities in Windows and Adobe Reader, and which, according to its own advertising, can be secretly installed on the target device. Once installed, Subzero takes 'full control of the target computer' and provides 'complete access to all data and passwords'. Subzero customers can extract passwords, take screenshots, view current and previous locations, and 'access, download, modify and upload files on the target computer' via a web interface. DSIRF promotes Subzero as 'next-generation cyber warfare', saying the tool was 'designed for the cyber age'[910]. In 2020 DSIRF valued its software Subzero at EUR 245 million.

---

[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 is an abbreviation for 'Decision Supporting Information Research and Forensic'.
[909] https://dsirf.eu/about/.
[910] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/.

511. The connection with Russia becomes clear from the links of several high level staff members of DSIRF. The owner of DSIRF is Peter Dietenberger, a ‘man with excellent connections in the Kremlin’ who ‘opens doors for western companies in Putin’s empire’[911]. Dietenberger lived in Russia for several years and had a Russian company and several Russian business partners. One of his Russian business partners, Boris Vasilyev, was also on the DSIRF board of directors. DSIRF provides several references for its firm and products: Michael Harms (CEO of the German Eastern Business Association), Stephan Fanderl (Chairman of the Board of Galeria Karstadt Kaufhof, who wanted to bring Walmart to Russia), Christian Kremer (former President of BMW in Russia and CEO of Russian Machines, which has been sanctioned by the US since 2018) and Florian Schneider (partner at the large business law firm Dentons in Moscow)[912]. Russian Machines, a company owned by the oligarch Oleg Deripaska, is said to use DSIRF’s services. Powerful local entrepreneur Siegfried ‘Sigi’ Wolf, who advised former Chancellor Sebastian Kurz on economic issues, is considered a confidante of Deripaska[913]. Jan Marsalek, an alleged criminal wanted on an Interpol arrest warrant for commercial fraud charges amounting to billions, among other financial and economic offences, is also involved. In August 2018, he received an email from Florian Stermann (Secretary General of the Russian-Austrian Friendship Society, considered in investigations by the public prosecutor’s office to be a ‘confidant’ of the FPÖ)[914] containing a DSIRF company presentation. In 2013, Marsalek allegedly tried to sell spyware produced by the Italian company Hacking Team to Grenada. He is said to be hiding in Moscow at the moment, under the care of the FSB, the Russian secret service[915].

512. In July 2022, Microsoft found out that Subzero was used during unauthorised, malicious activity to attack law firms, banks, and strategic consultancies in Austria, the United Kingdom and Panama[916]. Austria currently has no legal basis for the unauthorised deployment of spyware like Subzero by public authorities, and it would also be illegal for one private company to use it against another. Following the Microsoft publication, on 28 July 2022 the Austrian digital rights NGO Epicenter.works filed a criminal complaint against DSIRF at the Vienna Public Prosecutor’s Office for unlawful access to a computer system, data damage, interference with the functioning of computer systems, fraudulent misuse of data processing, criminal organisation and violation of the Foreign Trade and Payments Act with regard to dual-use goods[917]. On 7 October 2022, the Austrian Federal Ministry of Labour and Economic Affairs stated that it had not issued an export licence to DSIRF[918], and according to the Austrian Federal Ministry of

[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.
[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] Response by Martin Kocher, Federal Minister for Digital and Economic Affairs of Austria, to written parliamentary questions by Stephanie Krisper, 7 October 2022, reference 2022-0.575.143,

Justice, the Vienna Public Prosecutor's Office has started a criminal investigation into DSIRF[919]. The use of the Subzero spyware against targets in Austria means that a private or public authority in Austria has applied the software illegally, that the software was used by a foreign actor and export restrictions were violated by DSIRF, or that the software was exported to another Member State and used from there, be it legally or illegally, against an Austrian target. The investigation is still ongoing.

*FINFISHER*

513. The criminal investigation into and the bankruptcy of FinFisher, a former spyware company based in Munich, Germany, is also worth mentioning in this report. FinFisher is a company network founded in 2008 and originally had strong ties to the British network of companies operating under the Gamma brand. FinFisher promoted its spyware as a 'complete IT intrusion portfolio' and its software was used by dozens of countries all over the world[920], including 11 EU Member States[921] and 13 'not-free' countries[922].

514. In 2017, FinFisher's product FinSpy appeared in Turkey on a fake version of a mobilisation website for the Turkish opposition. The software was disguised as a downloadable app recommended to participants in anti-government demonstrations[923]. FinFisher itself advertised its products being used solely to fight crime. In 2019, a criminal complaint was filed against FinFisher by Gesellschaft für Freiheitsrechte, Reporter ohne Grenzen, the blog netzpolitik.org and the European Center for Constitutional and Human Rights for exporting its spyware without the necessary export licence from the German Federal Office for Economic Affairs and Export Control. It thereby violated the EU Dual-Use Regulation and the corresponding German national legislation. Following the complaint, the Munich Public Prosecutor's Office investigated FinFisher, and in October 2020 it searched 15 business premises of the FinFisher group in Germany and Romania, as well as private residences. In 2021, the Munich District Court approved the seizure by the Public Prosecutor's Office of FinFisher's bank accounts, in order to ensure that illegally obtained profits would be confiscated if FinFisher were convicted. However, FinFisher declared insolvency in February 2022. Its business operations have ceased, its office has been closed, and all 22 of its employees have been dismissed[924]. The criminal investigations into the people

---

https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml.

[919] Response by Alma Zadić, Federal Minister of Justice, to written parliamentary questions by Stephanie Krisper, 7 October 2022, Reference 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] Belgium, the Czech Republic, Estonia, Germany, Hungary, Italy, the Netherlands, Romania, Slovakia, Slovenia and Spain.

[922] Angola, Bahrain, Bangladesh, Egypt, Ethiopia, Gabon, Jordan, Kazakhstan, Myanmar, Oman, Qatar, Saudi Arabia and Turkey.

[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.

responsible for FinFisher's activities are still ongoing.

### *III. The European Union's capacity to respond*

515. Some governments have targeted EU citizens with powerful and highly invasive and intrusive spyware, abusing their right to resort to surveillance in case of risk to national security. This poses threats to democracy, the rule of law and the fundamental rights of individual citizens. The EU has few powers to act on these threats, and it turns out to be ill-equipped against potential criminal activity by national authorities, even if it affects the EU itself. Under the Treaties, national security remains the exclusive competence of the Member States but their actions must still comply with the fundamental rights and democratic norms embedded in EU law. Political factors also limit the EU's power to act. The European Commission, as guardian of the EU treaties, has not maximised its efforts at enforcing EU law by using legal instruments at its disposal. The Commission tends to interpret its powers very narrowly, as concerning almost exclusively the correct transposition of EU law into national law. The Commission considers that addressing transgressions of EU law is the sole responsibility of national authorities. When faced with flagrant violations of the rule of law and fundamental rights, this stance – which has no basis in the EU Treaties – becomes very problematic. Although subsidiarity and division of competences are a pillar of EU law, these should not lead to impunity for governments targeting EU citizens with spyware for political purposes. Below, we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce, and they have to do so with vigour and ambition, putting defence of our democracy over short-term political considerations.

*European Commission*

516. Following press reports about the use of spyware in Member States and questions by PEGA, Commission, in its response to the spyware scandal, has initially only written letters requesting clarification from the governments of Poland, Hungary, Spain, Greece, Cyprus and France. However, it would seem that this admonition by the Commission has not been followed by further action. It is true that strictly speaking, the Commission has no powers to act in the area of national security. However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness. It is up to the Member States, however, to 'demonstrate that national security would be compromised in the case at issue'. In response to the question of what actions the Commission will take if national authorities do not thoroughly examine any allegations of illegal spying, the Commission merely refers to the Court of Justice and to Article 47 of the Charter, which grants a right to an effective remedy before a tribunal. There seems to be no political willingness to act.

517. Moreover, on 21 December 2022, the Commission sent a general letter to all Member States, requesting information about the use of spyware by national authorities and the legal framework governing such use, for the purpose of a 'mapping of the situation in Member States' and examining 'the interplay with EU law'[925]. The Commission asked specific questions about, among other things, the purpose of use of spyware, the

[925] Letter DG JUST to Member States. Ref. Ares(2022)8885417, 21 December 2022.

authorities authorised to deploy it, the national definition of national security, relevant legislation that governs the processing of data for national security purposes, safeguards, prior authorisation by a court or independent administrative authority, oversight and notification, with a deadline of 31 January 2023 to respond. On 28 March 2023, Commissioner Reynders stated to PEGA that a large majority of the Member States had replied, but that the Commission was still in the process of collecting the Member State responses to this mapping exercise, and that it would 'carefully assess' the replies. Based on this mapping exercise, the Commission will reflect on its options regarding the use of spyware in Member States. However, no specific end date is envisaged for the Commission's assessment, 'given the evolving and sensitive nature of the assessment'. The Commission also mentioned that it would follow the findings of PEGA very closely.

518. Unlike the US, which has responded to the revelations by blacklisting companies, carrying out investigations, including on EU territory, and issuing an executive order prohibiting the acquisition of commercial spyware by US federal bodies, the Commission has so far not undertaken an analysis of the situation nor an assessment of the companies that are active on the spyware market within the EU. There is no obvious legal objection against conducting such an analysis. It is remarkable that the large amount of evidence has still not incited the Commission to take any meaningful action. Its inertia amounts to complicity in human rights violations and dereliction of duty.

519. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy[926]), there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission as Guardian of the Treaties is not performed to its full potential. It tends to limit itself to verifying if a Member State has correctly transposed EU laws into national law. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report[927] on the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. The implementation of the e-Privacy Directive and case-law deriving from it is poor. The Commission refers to the Member States as being responsible for implementation and enforcement, but it does not take action when Member States fail in these tasks. Without proper and meaningful enforcement, EU laws become ineffective and create ample space for the illegitimate use of spyware.

520. The Law Enforcement Directive was meant to provide high standards of data protection and ensure the free flow of data in the law enforcement and criminal justice sector. The directive had to be transposed into national law, with broad discretionary powers given to Member States. Today it is evident that implementation differs from Member State to Member State, especially in the area of data subjects' rights. The Commission should urgently assess the implementation in all Member States and identify the most serious

[926] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37).
[927] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

shortcomings. The Commission should develop concrete guidance to Member States on the directive's implementation in order to ensure that EU standards are respected across the Union. Furthermore, where necessary, the Commission should start infringement procedures in cases where the directive has not been transposed correctly and there is lack of willingness from the Member State to correct it.

*European Parliament*

521. The European Parliament has set up the PEGA committee of inquiry, which is working diligently and effectively within its powers and mandate. However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. It lacks the full investigative powers that most national parliaments have. In addition, the influence of national governments is frequently present in the deliberations of PEGA, which on occasion is an obstacle to thorough, fully independent and objective investigations. It is quite disturbing that the European Parliament does not have the full powers to investigate, when some of its own members have been targeted with spyware.

*European Council and Council of Ministers*

522. Although national governments claim that the spyware scandal is a purely national matter, it was actually discussed in the Council of the European Union and the national governments decided to respond collectively to the questionnaire of the European Parliament[928]. In doing so, they fully acknowledged that it is in fact a matter for the Council.

523. To date, the European Council has not responded publicly or substantively to the scandal. Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and powerless in this area.

524. Even if illegal or criminal behaviour were ultimately to be proven, members of national governments could not be impeached or made to resign from their EU jobs. This means that persons who are guilty of such acts may well continue with impunity to sit on EU bodies and take decisions affecting all European citizens.

*Europol*

525. Europol does not have any autonomous operational powers and it cannot act without the consent and cooperation of the Member State(s) concerned, as per Article 88(3) TFEU, while application of coercive measures are the exclusive responsibility of the competent national authorities. That presents a problem when there is clear evidence of criminal acts – such as cybercrime, corruption and extortion – but national authorities fail to investigate. Europol has recently obtained new powers allowing it to proactively propose an investigation, even when it concerns a crime committed only in one Member

[928] Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

State[929], but so far it has not made use of those powers.

526. On 28 September 2022, PEGA wrote a letter to Europol[930], urging it to make use of its new powers under Article 6 of the Europol Regulation[931]. In a letter of reply dated 13 October 2022[932], Europol stated that it had 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law)'. On 11 April 2023, Europol stated in a letter to PEGA that its letters had been sent to Greece, Hungary, Bulgaria, Spain and Poland. Following the response by the five Members States to Europol's letters, Europol mentioned that none of them had 'relevant information that is available for Europol'. By October 2022, one of the five Member States had confirmed to Europol 'the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. By December 2022, a second Member State had informed Europol 'that one criminal procedure was initiated in connection with the suspected unlawful use of Pegasus software which meanwhile was closed by the responsible judicial authorities in that country'. A third Member State notified Europol that 'pre-trial proceedings have been opened in one instance at the regional level', and inquired 'whether Europol holds information on the use of Pegasus software in the respective country, of relevance to the pre-trial proceedings.' A fourth Member State informed Europol 'that there is no criminal investigation ongoing or envisaged', but that 'judicial investigations had been initiated'. By April 2023, the fifth Member State had explained to Europol that 'following consultation of the competent authorities in that country, there is no relevant information available for Europol concerning the unlawful use of intrusive surveillance and interception software, while referring to preliminary proceedings of the public prosecutor's office'. It is not known whether the aforementioned criminal procedures by two Member States, pre-trial proceedings by one Member State, judicial investigations by one Member State, and preliminary proceedings of the public prosecutor's office in another Member State concern the abuse of spyware by EU Member State governments or by third countries.

527. The EU turns out to be quite powerless against potential criminal activity by national authorities, even if it affects the EU.

528. Paradoxically, contrary to Europol, the US is actively investigating the use of spyware in the EU. On 5 November 2022, it was reported that the FBI visited Athens to investigate 'how far the illegal surveillance has spread and who trafficked it.'[933]. Moreover, in March 2023, US President Biden issued an executive order largely

[929] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation (OJ L 169, 27.6.2022, p. 1).
[930] https://twitter.com/EP_PegaInquiry/status/1576855144574377984.
[931] 'Where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation.'.
[932] File no 1260379.
[933] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ.

prohibiting the use of spyware by US federal entities. A few days later, other countries, including France and Denmark, signalled their commitment to international cooperation on the topic.

*European judiciary*

529. The CJEU and the ECtHR play an important role in defending democracy, the rule of law and fundamental rights. However, they can only act upon a complaint or pre-judicial question. Proceedings are very lengthy and offer little concrete remedy in individual cases. Over the years, the courts have created a vast body of relevant case-law, for example establishing standards for surveillance. However, these courts have no means to ensure that their ruling are enforced. So far, one complaint about the illegitimate use of spyware has been submitted to the ECtHR[934]. However, the road to the Strasbourg or Luxembourg courts is often long, costly, and cumbersome, as all options for national judicial proceedings must first be exhausted. This is especially the case if national prosecutors or judges fail or refuse to take a case. The bar for passing the admissibility test is high.

*The Ombudsman*

530. On 28 November 2022, the EU Ombudsman concluded that the Commission had failed to sufficiently assess the human rights risks before providing support to African countries to develop surveillance capabilities, notably in the context of the EU Emergency Trust Fund for Africa (EUTFA). The conclusions followed a complaint by several civil society organisations. In Niger, the Fund allocated EUR 11.5 million for supplies of surveillance equipment, including surveillance software, a wiretapping centre, and an international mobile subscriber identity catcher[935], despite repression against activists in the country. To address the shortcomings she identified, the Ombudsman suggested improvements to ensure that a human rights impact assessment take place prior to future EUTFA projects.

*Other EU bodies*

531. The European Data Protection Board, the European Data Protection Supervisor, the European Court of Auditors and Eurojust have few competences to scrutinise or intervene in case of illegitimate use of or trade in spyware by Member State governments. Some of their members may indeed be involved in the scandals in their Member State of origin. This may have an impact on the functioning and the integrity of these EU bodies. The European Public Prosecutor's Office could potentially intervene when EU money is involved in any way.

[934] Appeal by Koukakis to the European Court of Human Rights, 27 July 2022.

[935] https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf.

## EXPLANATORY STATEMENT

### Europe's Watergate

In summer 2021, the Pegasus Project, a collective of investigative journalists, NGOs and researchers, revealed a list of 50,000 persons who had been targeted with mercenary spyware. Among them, journalists, lawyers, prosecutors, activists politicians, and even heads of state. The most dramatic case may well be that of Jamal Khashoggi, the Saudi journalist, who was savagely murdered in 2018 for his criticism of the Saudi regime. However, there were also many European targets on the list. Some had been targeted by actors outside the EU, but others were targeted by their own national governments. The revelations met with outrage around the world.

The scandal was quickly labelled "Europe's Watergate". However, rather than the political thriller "All the President's Men" about the burglary into the Watergate building in 1972, today's spyware scandal is reminiscent of the chilling movie "Das Leben der Anderen" (The Life of Others) depicting the surveillance of citizens by the totalitarian communist regime. Today's digital burglary with spyware is far more sophisticated and invasive, and hardly leaves any trace. The use of spyware goes far beyond the conventional surveillance of a person. It gives total access and control to the spying actors. Contrary to classic wiretapping, spyware does not only allow for real-time surveillance, but full, retroactive access to files and messages created in the past, as well as metadata about past communications. The surveillance can even be done at a distance, in countries anywhere in the world. Spyware can be used to essentially take over a smart phone and extract all its contents, including documents, images and messages. Material thus obtained can be used not only to observe actions, but also to blackmail, discredit, manipulate and intimidate the victims. Access to the victim's system can be manipulated and fabricated content can be planted. The microphone and camera can be activated remotely and turn the device into a spy in the room. All the while, the victim is not aware of anything. Spyware leaves few traces on the victim's device, and even if it is detected it is nearly impossible to prove who was responsible for the attack.

The abuse of spyware does not just violate the right to privacy of individuals. It undermines democracy and democratic institutions by stealth. It silences opposition and critics, eliminates scrutiny and has a chilling effect on free press and civil society. It further serves to manipulate elections. The term "mercenary spyware" reflects very well the nature of the product and of the industry. Even failed attempts to infect a smart phone with spyware have political ramifications, and can harm the individual as well as democracy. Participation in public life becomes impossible without the certainty of being free and unobserved.

The spyware scandal is not a series of isolated national cases of abuse, but a full-blown European affair. EU Member State governments have been using spyware on their citizens for political purposes and to cover up corruption and criminal activity. Some went even further and embedded spyware in a system deliberately designed for authoritarian rule. Other Member State governments may not have engaged in abuse of spyware, but they have facilitated the obscure trade in spyware. Europe has become an attractive place for mercenary spyware. Europe has been the hub for exports to dictatorships and oppressive regimes, such as Libya, Egypt and Bangladesh, where the spyware has been used against human rights activists, journalists and government critics.

The abuse of spyware is a severe violation of all the values of the European Union, and it is testing the resilience of the democratic rule of law in Europe. In the past years, the EU has very rapidly built up its capacity to respond to external threats to our democracy, be it war, disinformation campaigns or political interference. By contrast, the capacity to respond to internal threats to democracy remain woefully underdeveloped. Anti-democratic tendencies can freely spread like gangrene throughout the EU as there is impunity for transgressions by national governments. The EU is ill equipped to deal with such an attack on democracy from within. On the one hand the EU is very much a political entity, governed by supranational laws and supranational institutions, with a single market, open borders, passportless travel, EU citizenship and a single Area of Security, Freedom and Justice. However, despite solemn pledges to European values, in practice those values are still considered very much a national matter. The spyware scandal mercilessly exposes the immaturity and weakness of the EU as a *democratic* entity. With regard to democratic values, the EU is built on the "presumption of compliance" by national governments, but in practice, it has turned into "pretence of compliance". The scenario of national governments deliberately ignoring and violating the EU laws, is simply not foreseen in the EU governance structures. The EU has not been equipped with instruments for such cases. The EU bodies have few powers, and even less appetite, to confront national authorities in case of transgressions, and certainly not in the delicate area of "national security". By intergovernmental logic, the EU institutions are subordinate to the national governments. However, without effective, meaningful supranational enforcement mechanisms, new legislation will be futile. Fixing the problem will require both regulatory measures and governance reforms.

The US is not spared from attacks on democracy from the inside, for example Watergate, and the siege of Congress on January 6th 2021, but it is equipped to respond forcefully. It has the powers to confront even the highest political leaders when they do not respect the law and the Constitution.

Indeed, following the 2021 revelations on spyware, the United States responded rapidly and with determination to the revelations of the Pegasus Project. The US Trade Department swiftly blacklisted NSO Group, the Department of Justice launched an inquiry, and strict regulation for the trade in spyware is in the pipeline. The FBI even came to Europe to investigate a spyware attack against a dual US-European citizen. Tech giants like Apple and Microsoft have launched legal challenges against spyware companies. Victims have filed legal complaints, prosecutors are investigating and parliamentary inquiries have been launched.

In contrast, with the exception of the European Parliament, the other EU institutions have remained largely silent and passive, claiming it is an exclusively national matter.

The European Council and the national governments are practising omertà. There has not been any official response to the scandal by the European Council. Member State governments have largely declined the invitation to cooperate with the PEGA committee. Some governments downright refused to cooperate, others were friendly and polite but did not really share meaningful information. Even a simple questionnaire sent to all Member States about the details of their national legal framework for the use of spyware, has hardly received any substantial answers. Literally on the eve of the publication of this draft report, the PEGA

committee received a joint reply from the Member States via the Council, also without any substance.

The European Commission has expressed concern and asked a few Member State governments for clarifications, but only those cases where a scandal had already erupted at national level. The Commission has shared - reluctantly and piecemeal - information concerning the spyware attacks on its own Commission officials.

Europol has so far declined to make use of its new powers to initiate an investigation. Only after being pressed by the European Parliament, it addressed a letter to five Member States, asking if a police inquiry had started, and if they could be of assistance.

**Europe's business**

The abuse of spyware is mostly seen through the keyhole of national politics. That narrow national view obscures the full picture. Only by connecting all the dots, it becomes clear that the matter is profoundly European in all its aspects.

Although it is not officially confirmed, we can safely assume that all EU Member States have purchased one or more commercial spyware products. One company alone, NSO Group, has sold its products to twenty-two end-users in no fewer than fourteen Member States, among which are Poland, Hungary, Spain, The Netherlands and Belgium. In at least four Member States, Poland, Hungary, Greece, and Spain, there has been illegitimate use of spyware, and there are suspicions about its use in Cyprus. Two Member States, Cyprus and Bulgaria, serve as the export hub for spyware. One Member State, Ireland, offers favourable fiscal arrangements to a large spyware vendor, and one Member State, Luxemburg, is a banking hub for many players in the spyware industry. The home of the annual European fair of the spyware industry, the ISS World "Wiretappers Ball", is Prague in The Czech Republic. Malta seems to be a popular destination for some protagonists of the trade. A few random examples of the industry making use of Europe without borders:  Intellexa has a presence in Greece, Cyprus, Ireland, France and Hungary, and its CEO has a Maltese passport and (letterbox) company. NSO has a presence in Cyprus and Bulgaria and it conducts its financial business via Luxemburg. DSIRF is selling its products from Austria, Tykelab from Italy, FinFisher from Germany (before it closed down).

The trade in spyware benefits from the EU internal market and free movement. Certain EU countries are attractive as an export hub, as - despite the EU's reputation of being a tough regulator - enforcement of export regulations is weak. Indeed, when export rules from Israel were tightened, the EU became more attractive for vendors. They advertise their business as being "EU regulated", using, as it were, their EU presence as a quality label. "EU" grants respectability. EU membership is also beneficial for governments who want to buy spyware: EU Member States are exempt from the individual human rights assessment required for an export license from the Israeli authorities, as EU membership is considered sufficient guarantee for compliance with the highest standards.

The sales side of the trade in spyware is opaque and elusive, but lucrative and booming. Company structures are conveniently, if not deliberately, complex to hide from sight undesirable activities and connections, including with EU governments. On paper the sector is regulated, but in practice it manages to circumvent many rules, not least because spyware is a

product that may serve as political currency in international relations. Spyware companies are established in several countries, but many have been set up by former Israeli army and intelligence officers. Most vendors claim they sell only to state actors, although backstage, some also sell to non-state actors. It is virtually impossible to get any information about those customers, or about the contractual terms and compliance.

Trade in, and use of spyware fall squarely within the scope of EU law and case-law. The purchase and sale of spyware is governed by i.a. procurement rules and export rules such as the Dual Use Regulation. The use of spyware has to comply with the standards of the GDPR, EUDPR, LED and e-Privacy Directive. The rights of targeted persons are laid down in the Charter on Fundamental Rights and international conventions, notably the right to privacy and the right to a fair trial, and in EU rules on the rights of suspects and accused. The abuse of spyware will in many cases constitute cybercrime, and it may entail the crimes of corruption and extortion, all of which fall within the remit of Europol. If European funds are involved, the European Public Prosecutor has the mandate to act. The abuse of spyware may also affect police and justice cooperation, notably the sharing of information and implementation of the European arrest warrant and the Evidence Warrant.

The abuse of spyware affects the EU and its institutions directly and indirectly. Amongst those targeted with spyware, there were members of the EU Parliament, of the European Commission and of the (European) Council. Others were affected as "by-catch", indirect targets. Inversely, some of the "perpetrators" also sit on the (European) Council. In addition, manipulation of national elections with the use of spyware, directly affects the composition of EU institutions and the political balance in the EU governance bodies. The four or five governments accused of abusing spyware, represent almost a quarter of the EU population, so they carry considerable weight in the Council.

**Spyware as part of a system**

Spyware is not a mere technical tool, used ad hoc and in isolation. It is used as integral part of a system. In principle its use is embedded in a legal framework, accompanied by the necessary safeguards, oversight and scrutiny mechanisms, and means of redress. The inquiry shows that these safeguards are often weak and inadequate. That is mostly unintentional, but in some cases, the system has - in part or in whole - been bent or designed purposefully to serve as a tool for political power and control. In those cases, the illegitimate use of spyware is not an incident, but part of a deliberate strategy. The rule of law turns into the law of the ruler. The legal basis for surveillance can be drafted in in vague and imprecise terms, so as to legalise broad and unfettered use of spyware. *Ex-ante* scrutiny in the form of judicial authorisation of surveillance can easily be manipulated and gutted of any meaning, in particular in the case of politicisation, or state capture of the judiciary. Oversight mechanisms can be kept weak and ineffective, and brought under control of the governing parties. Legal remedy and civil rights may exist on paper, but they become void in the face of obstruction by government bodies. Complainants are refused access to information, even regarding the charges against them that supposedly justified their surveillance. Prosecutors, magistrates and police refuse to investigate and often put the burden of proof on the victims, expecting them to prove they have been targeted with spyware. This leaves the victims in a Catch-22 situation, as they are denied access to information. Government parties can tighten their grip on public institutions and the media, so as to smother meaningful scrutiny. Public or commercial media close to the government can serve as the channel for smear campaigns

using the material obtained with spyware. "National security" is frequently invoked as a pretext for eliminating transparency and accountability. All these elements combined form a system, designed for control and oppression. This not only leaves individual victims completely exposed and defenceless against an all-powerful government, it also means all vital checks and balances of a democratic society have been disabled.

Some governments have already reached this point, others are halfway there. Fortunately, most European governments will not go down this road. However, when they do, the EU in its current institutional and political set up, is not equipped to prevent or counter it. Spyware is the canary in the coal mine: exposing the dangerous constitutional weaknesses in the EU.

**Secrecy**

A major obstacle in detecting and investigating the illegitimate use of spyware is secrecy.

For most victims it is not possible to get any information about their case from the authorities. In many cases the authorities refer to national security grounds as justification for secrecy, in other cases they simply deny the existence of a file, or the files are destroyed. At the same time, prosecutors frequently refuse to investigate these cases, arguing that the victims do not have sufficient evidence. This is a vicious circle that leaves victims without recourse.

Governments most often refuse to disclose whether they have bought spyware and what type. Spyware vendors equally refuse to disclose who their customers are. Governments often resort to middlemen, proxies or personal connections, to purchase commercial spyware or spyware-related services, so as to conceal their involvement. They circumvent procurement rules and budget procedures, so as to not leave any government fingerprints.

Israel is an important hub of spyware companies, and responsible for issuing marketing and export licenses. Although Israel and Europe are close allies, Israel does not give out any information about the issuance (or repeal) of licenses for spyware to EU countries, despite the fact that it is being used to violate the rights of European citizens and to undermine our democracy.

Freedom of information requests by journalists yield little to no information. Dedicated scrutiny and oversight bodies, like the data protection authorities or the court of auditors, are struggling as well to get information. Independent oversight over secret services is notoriously weak and often non-existent. Parliamentary inquiry committees are often stonewalled by the government parties. Judicial inquiries focus on hacks by third countries, not on illegitimate use by EU governments. Journalists reporting on the issue are facing strategic lawsuits against public participation (SLAPPs), verbal attacks by politicians or smear campaigns. The courageous and diligent journalists who are unearthing the facts of the scandal deserve our respect and gratitude. They are Europe’s Woodwards and Bernsteins. Furthermore, adequate whistleblower protection is still not in place in all Member States. In some cases victims of a spyware attack themselves wish to remain silent, as they do not wish to expose the parties behind the attack, for fear of retaliatory actions, or of the consequences of compromising material coming to the surface.

**Next steps**

At a time when European values are under attack from an external aggressor, it is all the more important to bolster our democratic rule of law against attacks from the inside. The findings of the PEGA inquiry are shocking and they should alarm every European citizen. It is evident that the trade in, and use of spyware should be strictly regulated. The PEGA committee will make a series of recommendations to that effect. However, there should equally be initiatives for institutional and political reforms enabling the EU to actually enforce and uphold those rules and standards, even when they are violated by Member States themselves. The EU has to rapidly develop its defence lines against attacks on democracy from within.

## INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE

| | |
|---|---|
| **Date adopted** | 8.5.2023 |
| **Result of final vote** | +: 30<br>–: 3<br>0: 4 |
| **Members present for the final vote** | 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 |
| **Substitutes present for the final vote** | Andrzej Halicki, Gabriel Mato, Thijs Reuten, Jordi Solé, Yana Toom |
| **Substitutes under Rule 209(7) present for the final vote** | Aurélia Beigneux, Theresa Bielowski, Franc Bogovič, Catherine Griset, Andreas Schieder |

## FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

| 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 |
| The Left | 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 |

Key to symbols:
+ : in favour
- : against
0 : abstention