

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

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))

Rapporteur: Sophie in 't Veld

Document of compromises

Table of Contents

Compromises on General Introduction	2
Compromises on Poland.....	6
Compromises on Hungary.....	32
Compromises on Greece	50
Compromises on Cyprus	84
Compromises on Spain.....	102
Compromises Other Member States	128
Compromises EU Institutions.....	150
Compromises on Third Countries.....	154
Compromises Spyware Industry.....	161
Compromises on the European Union's capacity to respond.....	181

Compromises on General Introduction

(Paragraph -1 a (new) to Paragraph -1 p (new))

Covered: 14 (S&D), 17 (S&D), 18 (S&D), 19 (S&D), 20 (S&D), 21 (S&D), 22 (S&D), 23 (S&D), 25 (S&D), 26 (S&D), 27 (S&D), 28 (S&D), 30 (S&D), 718 (Greens), 719 (rapporteur), 897 (rapporteur), 898 (EPP), 899 (ECR), 906 (EPP), 1047 (EPP), 1049 (EPP), 1052 (EPP), 1053 (EPP)

Falls: 29 (S&D), 900 (ID), 901 (ECR), 902 (EPP), 903 (EPP), 904 (ECR)

General Introduction

-1 a (new). In July 2021, a collective of investigative journalists, NGOs and researchers - the Pegasus Project - published a report based on 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 authoritarian as well as by democratic governments around the world with and without judicial oversight to target journalists, lawyers, judges, activists, politicians and state officials. In the European Union as well, persons were targeted with spyware: sometimes by actors outside the EU, others by actors within, 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 of abuse of spyware in several Member States for purely political purposes, targeting critics and opponents of the parties in power, or in connection to corruption. Investigative findings link Pegasus and other surveillance spyware to various human rights violations by governments, ranging from monitoring, blackmailing, smear campaigns, intimidation and harassment. It raises concerns on 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, abuse of spyware for political purposes is extremely alarming and raise very serious concerns over the procedural and substantive lawfulness of surveillance practices and the level of protection granted by European and national law (25). Such spyware abuses directly undermine fundamental rights and democracy, the core values on which the EU is founded (21). Subsequent investigative media reports and other sources have demonstrated that, in blatant breach of EU export rules, spyware is being exported from EU countries to third countries with undemocratic regimes and a high risk of human rights violations. The spyware industry is firmly established in the EU, benefiting from very favourable conditions for businesses.

-1 b (new). 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 (14), to investigate alleged contraventions, or maladministration in the implementation, of Union law as regards the use of the Pegasus and equivalent surveillance spyware, abbreviated to 'PEGA' (17). 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 (18), 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 (19).

-1 c (new). 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, also the definition of ‘cyber-surveillance items’ as laid down in the Dual Use Regulation was used, which describes these 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 on the Media Freedom Act, 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.’ (22)

-1 d (new). On 19 April 2022, the Committee of Inquiry began its work, and gathered information by means of public hearings, missions, consultation of experts, requests for data, evidence, and research (20)

-1 e (new). 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^{1a}. Spyware can be installed in mobile phones of pre-identified individuals at a distance, also across countries. 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 updates. The infected device then transmits the collected data from the device and enables operators not only 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.

-1 f (new). 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, as well as metadata about past communications. As a result, a judicial decision on an entry date and duration of the surveillance operation, provides ineffective safeguards when spyware grants full retroactive access to data with the means of spyware. 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 (23).

Footnote:

-1 g (new). The PEGA committee has received minimal or no ~~meaningful information~~ 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 the customers. Many Member States authorities have not provided PEGA with meaningful information about the legal frameworks governing the use of spyware and the use of spyware in their Member States beyond what was already publicly known (897), mainly due to national legal requirements of secrecy and confidentiality (28).

-1 h (new). Some Member States have deployed spyware and refused to comment on it by invoking national security, which, according to Article 4(2) TEU, "remains the exclusive competence of each EU Member State" (26). However, case law of the CJEU and ECtHR states that national security considerations national security have to be reconciled with 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', 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, missions, and following information requests. The lack of clarity as to how national security is defined, and an excessively broad interpretation of its scope by the national authorities, poses a challenge in understanding the justification for the use of spyware (27).

-1 i (new). 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.

-1 j (new). 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.

-1 k (new). From information provided by NSO Group, it is known that Pegasus was sold in at least fourteen EU countries, until the contracts with two countries were terminated. It is

not know which, but there is a general assumption it concerns Poland and Hungary. However, as long as NSO Group or the Israeli government does not make any official statement regarding a termination of contract, it cannot be verified if this is true.

-1 l (new). An additional piece of information is the attendee list of the 2013 edition of the ISS World (Intelligence Support Systems) fair, aka ‘The Wiretappers Ball’. With the exception of Portugal and Luxemburg, all current EU Member States were represented by a wide range of organisations, including local police forces^{1a}. In recent years, NSO Group has become the main sponsor of the event, but the sponsor list also mentions Intellexa, Candiru, RCS and many others^{1b}.

Footnotes:

1a <https://wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf>

1b https://www.issworldtraining.com/iss_europe/sponsors.html

-1 m (new). Member States are not just customers of commercial spyware vendors, they also have other, different roles in the spyware trade. Some are host to spyware vendors, some are the preferred destination for finance and banking services, others yet offer citizenship and residency to protagonists of the industry.

-1 n (new) 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 on certain countries regarding their permissive intelligence frameworks, ineffective checks, lax oversight practices and political interference (30)

-1 o (new). 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 the investigation methods without proper judicial control. Depending on the national legislation, the use of spyware is legitimate in investigations under judicial oversight (906).

-1 p (new). 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. Within the EU there has been very little action so far. There must be clear rules for the use of, and trade in spyware, preferably in tandem with other countries, such as the US.

Compromises on Poland

COMP 1 (paragraph 1 to paragraph 3 g (new))

Covered : 34 (ID), 41 (RE), 42 (Greens), 43 (rapporteur), 44 (EPP), 45 (rapporteur), 46 (Greens), 47 (rapporteur), 48 (Greens), 49 (Greens), 50 (rapporteur), 51 (Greens), 52 (rapporteur), 53 (rapporteur), 54 (Greens), 55 (rapporteur), 56 (Greens), 57 (Greens), 58 (rapporteur), 59 (rapporteur), 134 (Greens), 135 (Rapporteur)

Falls : 31 (EPP) 32 (ECR), 33 (EPP), 35 (EPP), 36 (ECR), 37 (EPP), 38 (ID), 39 (ECR), 40 (EPP), 123 (ECR), 125 (ID)

I. The use of spyware in the EU

I.A Poland

1. The representatives of the ministries approached declined to meet the delegation of the committee. In response to the questionnaire sent out by the PEGA Committee 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^{1a}. The Minister of the Interior, Mariusz Kaminski, also refused to accept an invitation by the PEGA Committee to exchange views^{1b}.

Footnotes:

1a Response by the Permanent Representative of Poland to the EU, Andrzej Sadós, to the PEGA Committee, 7 September 2022.

1b Response by Minister of the Interior, Mariusz Kaminski, by letter to the PEGA Committee, 12 July 2022.

2. The PEGA Committee'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 the 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.

~~1. The use of commercial spyware in Poland first came to the broad attention of the public in December 2021. Its dangers can only be wholly understood in its full context. Commercial spyware is not merely a technical instrument used in isolation and in random situations. It is an integral and vital part of a system designed specifically for the unfettered surveillance and control of citizens. The legal, institutional and political building blocks of this system were purposefully and methodically put together to create a coherent and highly effective framework. The complete image of this carefully planned system only becomes visible by connecting the dots.~~

~~2. The scope for legal surveillance in Poland has been expanded to the near unlimited. The rights of victims have been minimised and legal remedy has been rendered meaningless in practice. Effective ex-ante and ex-post scrutiny, as well as independent oversight, have been all but eliminated. Members of the Polish government and party loyalists control, directly or indirectly, the main positions within the system. The information harvested with spyware is used in smear campaigns against government critics and opposition, through the government-controlled state media. All safeguards have been eliminated, the government parties have full control and victims have nowhere to turn.~~

Purchase of Pegasus

3. In November 2016, former Prime Minister and current MEP Beata Szydło and former Foreign Minister Witold Waszczykowski, attended dinner at the home of ~~then~~-Israeli Prime Minister Benjamin Netanyahu². The following year in July, Szydło and Netanyahu met with the heads of governments of the Visegrád 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'³. 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 Netanyahu⁴. Despite initial denials, in January 2022 PiS leader Jarosław Kaczyński confirmed the purchase of spyware by the Polish government⁵⁻⁶⁻⁷.

Footnotes:

2 Gazeta, <https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html>, 29 January 2022.

3 Gazeta, <https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html>, 29 January 2022.

4 Financieele Dagblad, 'De wereld deze week: het beste uit de internationale pers', 7 January 2022.

3 a (new). *Initially, the Polish Government and PiS leader Jarosław Kaczyński denied the purchase of Pegasus^{1a}. However, in early January 2022, they confirmed the purchase of spyware by the Polish Government^{1b 1c 1d}. 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^{1e}. 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^{1f}. Kwiatkowski testified that the NIK had discovered accounts from the National Bank of Poland certifying the transfer^{1g}. (45, 46)*

Footnotes:

1a <https://www.politico.eu/article/poland-government-scrambles-minimize-hacking-backlash/>.

1b Financieele Dagblad, 'Liberalen Europarlement eisen onderzoek naar spionagesoftware', 12 January 2022.

1c Politico, <https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/>.

1d January 2022, Financial Times, <https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e>, 8 February 2022.

1e Business Insider, <https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1>, 18 January 2022.

1f 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.

1g 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.

3 b (new). *The invoices were issued by Matic Sp. z o.o., which acted as an intermediary through which the CBA carried out this purchase^{1a}. 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^{1b}.*

Footnotes:

1a Gazeta Wyborcza, <https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html>, 17 January 2022.

1b <https://ipn.gov.pl/en/about-the-institute>.

3 c (new). *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^{1a}. 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^{1b}. (49, 50) Representatives of Matic declined to meet and share information with the committee of inquiry.*

Footnotes:

1a Gazeta Wyborcza, <https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinnafirma-ludzi.html>, 17 January 2022.

1b Gazeta Wyborcza, <https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinnafirma-ludzi.html>, 17 January 2022.

3 d (new). *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, which is not part of the state budget but a public fund earmarked for victims of crime^{1a}. 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^{1b}. 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^{1c} and a close associate of the Minister of Justice, Zbigniew Ziobro^{1d}. 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’^{1e}. It therefore appears that they were misled by the government. (41, 53, 54). 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 Office of the Prosecutor will take action on such a case, given the current institutional and political environment. (134, 135)*

Footnotes:

1a 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, Poland Specific Chapter, 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.

1b Business Insider, <https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1>, 18 January 2022.

1c 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.

1d Gazeta Wyborcza, <https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html>, 4 January 2022.

1e <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.

3 e (new). *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. (55, 56)

3 f (new). *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^{1a}. 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^{1b}. 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, this has not been confirmed. (57, 58)*

Footnotes:

^{1a} Discussion with NSO Group, Mission of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware to Israel, July 2022.

^{1b} Testimony by Chaim Gelfand, General Counsel and Chief Compliance Officer, NSO, in PEGA 21 June 2022.

3 g (new). *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 European Court of Human Rights (ECtHR)^{1a}. (59)*

Footnote:

^{1a} PEGA Committee meeting, 19 January 2023.

COMP 2 (paragraph 4 to paragraph 4 b (new))

Covered: 61 (RE), 63 (EPP), 64 (rapporteur), 65 (EPP), 70 (Greens), 71 (rapporteur), 74 (rapporteur), 75 (Greens)

Falls: 60 (Renew), 62 (ECR), 72 (EPP), 73 (EPP)

Legal framework

4. 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 ~~Polish~~ Constitution **of Poland**⁸ (61). The Tribunal concluded by issuing a judgement containing specific recommendations and an 18-month timeline within which legislative changes were to be implemented⁹. 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 had been required by the Constitutional Court¹⁰. Instead, the 2016 Police Act has weakened the ~~already lackluster~~ **existing** provisions ~~that do not protect the~~ **which in themselves had neither sufficiently protected the** rights of citizens ~~or create~~ **nor created** proper

oversight and compounded the ever-growing distance between the Polish legislature and the rule of law.

Footnotes:

- 8 Venice Commission Report June 2016,
[https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2016\)012-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e)
9 <https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostceza-pomoca-srodkow-technicznych-w-dzialani>.
10 Act of 15 January 2016 Amending the Police Act and certain other acts at Article 20(c), <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

4 a (new). *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’^{1a}. Moreover, the lack of specificity regarding oversight, guarantees against abuse and the categories of persons and crimes that could be targeted also violate the judgements of ECtHR^{1b}. In particular, in the judgement 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^{1c}. Moreover, the court explicitly stated that it would be ‘contrary to the rule of law’ if discretion regarding secret surveillance was concentrated entirely with the executive of the judiciary^{1d}. 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 judgement. (70, 71)*

Footnotes:

- 1a 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.
1b 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.
1c Roman Zakharov v. Russia [GC], no. 47143/06, ECtHR, judgment of 4 December 2015.
1d Roman Zakharov v. Russia [GC], no. 47143/06, ECtHR, judgment of 4 December 2015, in paragraphs 229 and 230. See also Venice Commission Report June 2016, [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2016\)012-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e), p. 11.

4 b (new). *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’^{1a} 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 (74, 75)^{1b}. At the same time, the government has declined all requests for dialogue and clarification about how surveillance is used in Poland.*

Footnotes:

- 1a Klass and others v. Germany, 6 September 1978, paragraph 50, Series A no. 28. 40.
1b Letter from Mariusz Kaminski, Minister of the Interior and Administration of Poland, to the PEGA Committee, 8 September 2022.

COMP 3 (Paragraph 5)

Paragraph 5

Covered: 78 (EPP), 80 (ID), 81 (RE), 82 (rapporteur)

Falls: 77 (EPP), 79 (ECR),

Anti-Terrorism Law 2016

5. In addition to the 2016 Police Act, the *Sejm* ~~Polish government~~ also adopted a law governing the surveillance of foreign citizens in 2016 that it dubbed the ‘Anti-Terrorism law’. ~~The articles of the Act~~ ***It*** stipulates that non-Polish citizens can be monitored without ~~their~~ ***the court’s*** consent for a period of three months if their identity is ‘doubtful’, including through ~~the~~ wiretapping of phones, ~~the~~ collection of fingerprints, biometric photos and DNA, and the obligation to register pre-paid phone cards¹¹. ***According to the Article 9.8. of the act***, the Prosecutor-General ***has the power to order*** ~~is responsible for ordering~~ the destruction of non-relevant materials. ***Given the fact that*** Zbigniew Ziobro, ***who is also*** the PiS Minister of Justice, currently holds ~~that office~~ ***this position***, ***there are serious concerns as to whether he is capable of taking independent and impartial decisions without being biased by the political interests of the government which he represents***^{12 13}.

Footnotes:

11 Act of 10 June 2016 on Anti-terrorism Operations, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf>.

12 Act of 10 June 2016 on Anti-terrorism Operations, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf>.

13 European Digital Rights (EDRi), <https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/>, 29 June 2016.

COMP 4 (Paragraph 6)

Paragraph 6

Covered: 83 (RE), 84 (EPP)

Falls: 85 (ECR)

Code of Criminal Procedure

6. 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 rewritten in March 2016 in order to include Article 168a¹⁴. This addition now ensures that evidence gathered in violation of the law, or ‘fruit of the poisonous tree’, such as information harvested through the use of Pegasus, is eligible to be ~~introduced before the court~~, ***used in criminal proceedings***¹⁵. ***However, it must be added that the Supreme Court of Poland indicated in its judgment that this article cannot be applied in contradiction with the provisions of the European Convention on Human Rights and the Constitution of Poland, which in some cases limits its effective application***^{15a}. ***Judgments have also been issued in which Article 168a has been found partially***

unconstitutional^{15b}. Nevertheless, the presence of this provision in the legal system raises uncertainty when it comes to respect for fundamental rights.

Footnotes:

14 Act of 11 March 2016 amending the Act – Code of Criminal Procedure and certain other acts
<https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000437/T/D20160437L.pdf>

15 <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>.

15a For example, Judgment of the Supreme Court of Poland of 26 June 2019, IV KK 328/18.

15b For example, Judgment of the Supreme Court of Poland of 26 June 2019, IV KK 328/18.

COMP 5 (Paragraph 7 to Paragraph 7 d (new))

Paragraph 7

Covered: 86 (EPP), 87 (EPP), 90 (rapporteur), 91 (EPP), 92 (Greens), 93 (rapporteur), 94 (RE), 95 (rapporteur)

Falls: 88 (ECR), 89 (ID)

Telecommunications Law of 16 July 2004

7. *After the 2016 amendment to the Telecommunications Act of 2004, the law governing telecommunications in Poland includes provisions for allowing the police to gain **unrestricted** access to **metadata** telecommunication data for free and, in certain cases, **to do so** without the **involvement** participation of employees of the telecommunications companies¹⁶. Such access can be **done obtained** under the vague **a very broad** justification of ‘**discovering prevention or detection of crimes**’. The prosecutor then decides how to proceed **upon** receipt of this data and indeed is given a significant amount of power in the Act, which is a political decision. **This cannot be regarded as a safeguard, however, given that Ziobro is in that role 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**¹⁷. (87, 90)*

Footnotes:

16 Telecommunications Act of 16 July 2004, <https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004>.

17 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>.

7 a (new). *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^{1a}. (92, 93, 94)*

Footnote:

1a 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.

The Act implementing the Law Enforcement Directive

7 b (new).

Poland has not properly implemented the Law Enforcement Directive (EU) 2016/680^{1a}, 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 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^{1b}.

Footnotes:

1a 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).

1b 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](https://bip.brpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20(OSIOD%C5%81A%C4%86%20PEGAZA).pdf).

7 c (new). 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 Court of Justice of the European Union (CJEU)^{1a}. (144, 145)

Footnote:

1a https://ec.europa.eu/commission/presscorner/detail/en/ip_23_703

7 d (new). The Sejm, in particular members of the PiS Party, 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^{1a}. (95)

Footnote:

1a Euractiv, Polish government working on controversial surveillance bill, <https://www.euractiv.com/section/politics/news/polish-government-working-on-controversial-surveillance-bill/>.

COMP 6 (Paragraph 8 to Paragraph 8 c (new))

Paragraph 8

Covered: 96 (RE), 99 (EPP), 100 (EPP), 102 (Greens), 103 (rapporteur), 104 (Greens), 105 (rapporteur), 106 (Greens), 107 (rapporteur), 108 (Greens), 109 (rapporteur),
Falls: 97 (ECR), 98 (ID), 101 (Renew)

Ex ante scrutiny

8. Although, **as a rule**, surveillance **in Poland** requires judicial authorisation ~~in principle in Poland, in practice~~ the **existing** authorisation procedure ~~no longer~~ **does not serve** as a safeguard against abuse, but rather as a means to lend a veneer of legality to surveillance **used** for political purposes. It has not been made explicitly clear whether any of the victims of Pegasus to date were spied on with judicial authorisation. Applications for judicial authorisation of a surveillance operation are submitted by the special services¹⁹. 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 submitted²⁰. The information is often merely a summary, sometimes excluding even the most basic details regarding the **targeted person** (name, profession, the crime of which ~~he/she is~~ **they are** suspected) and a **description** of the surveillance methods to be used. **(96, 100)**

Footnotes:

19 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>.

20 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>.

8 a (new). *If a judge rejects an application, they are required to give a reasoned justification for such a decision and it can be subject to appeal^{1a}. 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^{1b}. This is a significant and deliberate loophole in the Polish legal framework. (104, 105)*

Footnotes:

1a <https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef>.

1b <https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef>.

8 b (new). *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. (106, 107, 99)*

8 c (new). *Several dozen surveillance applications are submitted every day, stretching the capacity of the court to conduct an in-depth examination of each request^{1a}. 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^{1b}. 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^{1c}. 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’^{1d}. (108, 109). All this severely undermines the capacity of the court to perform effective judicial oversight (99).

Footnotes:

1a Testimony of Ewa Wroszek, 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.

1b Testimony of Ewa Wroszek, 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.

1c Testimony of Ewa Wroszek, 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.

1d Testimony of Ewa Wroszek, 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.

COMP 7 (Paragraph 9 to paragraph 9 c (new))

Paragraph 9

Covered: 112 (RE), 113 (EPP), 114 (RE), 115 (Greens), 116 (rapporteur), 117 (Greens), 118 (rapporteur), 119 (Greens), 120 (rapporteur), 121 (Greens), 122 (rapporteur), 167 (Greens), 168 (rapporteur)

Falls: 110 (ID), 111 (ECR)

Ex post scrutiny

9. Parliamentary oversight is virtually non-existent in Poland. ~~When PiS came to power in 2015, the traditional system of the opposition party taking on the Chairmanship of~~ **Before 2016**, the Parliamentary Oversight Committee for the Special Services (KSS) was ~~rejected~~ **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 Chairman **of this committee**²¹. The government parties have the absolute majority in the committee²². **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^{23 24 25 26 27}. The Senate on the other hand, where the government parties hold no majority, ~~did~~ set up an inquiry committee **in early 2022. But** **However**, the Senate **committee** lacks the **investigative** powers of inquiry of the Sejm, **whose inquiry committee can summon witnesses and hear sworn testimony.** (112, 113) **The committee has been opposed at every turn by the ruling party in the Sejm**^{27a}, **government officials and security agencies, all of which have refused to cooperate or conduct their own investigation**^{27b} (167, 168).

Footnotes:

21 <https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS>.

22 <https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS>.

- 23 AP, <https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422>, 17 January 2022.
- 24 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.
- 25 AP, <https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab>, 23 December 2021.
- 26 The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', 24 January 2022.
- 27 Politico, <https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/>, 18 January 2022.
- 27a 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.
- 27b AP, <https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422>, 17 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. 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.

9 a (new). *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^{1a}. The Sejm has so far failed to appoint 10 of the 19 members of the NIK Council^{1b}. The required vetting of council members carried out by the special services, headed by Minister Kaminski, is very slow^{1c}. (115, 116)*

Footnotes:

1a 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.

1b <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.

1c 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.

9 b (new). *When a violation of the law is discovered by the NIK, they have the power to submit a notification to the Prosecutor's Office^{1a}. 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 Office of the Prosecutor 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 that had been terminated by the prosecution service. He can also initiate disciplinary proceedings against prosecutors whom he suspects of having taken wrong decisions. (117, 118).*

Footnote:

1a 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> at Article 63.

9 c (new). *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^{1a}. 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^{1b}. (121, 122)*

Footnotes:

1a Euractiv, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/, 22 July 2021.

1b Study – Europe’s PegasusGate: Countering spyware abuse, European Parliament. Directorate-General for Parliamentary Research Services, 6 July 2022, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU\(2022\)729397_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf), p. 22.

COMP 8 (Paragraph 10)

Paragraph 10

Covered: 124 (EPP)

Falls: 123 (ECR), 125 (ID)

Reporting

10. Under the 2016 Police Act, **the** police are only required to submit ~~semi-annual~~ 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 the **prevention or detection of crimes**, protection of human life or health, or supporting search and rescue **operations**)²⁹. These reports can only be ~~done~~ **carried out ex post** and are not made public. If there is an issue with the submission, the court will submit ~~their~~ **its** findings in response within 30 days, but ~~they~~ cannot order the destruction of any data even if ~~they~~ it finds incompatibilities with the law. ~~Critically~~ **Most importantly**, these supervisory actions are only optional, not mandatory. (124)

Footnote:

29 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>.

COMP 9 (Paragraph 11 to paragraph 11 f (new))

Paragraph 11

Covered: 129 (EPP), 130 (rapporteur), 131 (Greens), 132 (Greens), 133 (rapporteur), 134 (Greens), 135 rapporteur), 136 (Greens), 137 (rapporteur), 138 (rapporteur), 139 (Greens), 140 (rapporteur), 141 (Greens), 142 (Greens), 143 (rapporteur), 144 (rapporteur), 145 (Greens)
Falls: 126 (ID), 127 (ID), 128 (ECR)

Redress

11. So far, ~~the Polish Prosecutor has not launched an inquiry~~, 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*** ~~has~~ been taken up by the courts. Wrzosek initially filed her case with the Office of the Prosecutor; however, upon ~~their~~ ***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, such as gathering testimony from the victim, necessary for the cases to progress (129).***

11 a (new). 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 Office of the Prosecutor. 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. (130, 131)

11 b (new). Citizens who have been targeted can bring a civil case before court, but the burden of 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. (132, 133)

11 c (new). 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^{1a} who submitted complaints to the ECtHR in September 2017 and February 2018 respectively. Eleven entities submitted amicus curiae briefs in this case, including European Criminal Bar Association^{1b}, the Polish Ombudsman, and the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism^{1c}. (136, 137)

Footnotes:

^{1a} 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 Panoptikon Foundation based in Warsaw.

1b <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>.

1c https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/SR/AmicusBrief_Poland_SRCT_ECHR.pdf.

11 d (new). 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. (138, 139)

11 e (new). 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. (140, 141)

11 f (new). 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 subjected to secret surveillance and, if necessary, to have the lawfulness of that surveillance reviewed by a court. (142, 143)

COMP 10 (Paragraph 12)

Paragraph 12

Covered: 148 (EPP), 149 (EPP)

Falls: 146 (ID), 147 (ID), 150 (ECR)

Public Scrutiny

12. *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 smart phones of several of the targets, including *the opposition* Senator *Krzysztof* Brejza. Making

public information obtained in a surveillance operation of the special services is a criminal act in itself. Yet, no action has been taken by the police or the public ~~prosecution~~ **prosecutor**.

COMP 11 (Paragraph 13 to 13 c (new))

Paragraph 13

Covered: 152 (EPP), 154 (rapporteur), 155 (Greens), 156 (Greens), 157 (rapporteur), 158 (rapporteur), 159 (Greens), 160 (Greens), 161 (rapporteur)
Falls: 151 (ID), 153 (ECR)

Political Control

13. 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' imprisonment³². ~~But~~ **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. It raises concerns about his independence and neutrality. ~~Mr~~ Kaminski has declined to meet with or cooperate **in a substantial manner** with the PEGA ~~European Parliament Pegasus Special Inquiry Committee~~³³.

Footnotes:

32 Reuters, <https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117>, 17 November 2015.

33 EU Observer, <https://euobserver.com/rule-of-law/156063>, 15 September 2022.

13 a (new). *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^{1a}, and which states in Article 1.1 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'^{1b}. In the 2022 Annual Rule of Law Report, the Commission finds that 'The 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'. (156, 157)*

Footnotes:

1a https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf.

1b https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf, at Article 1.1.

13 b (new). *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. (158, 159)*

13 c (new). *Not only has the legal and institutional context been created to enable near unlimited 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. (160, 161)

COMP 12 (Paragraph -14 new to paragraph 14 c (new))

Paragraph 14

Covered: 163 (rapporteur), 164 (EPP), 165 (Greens), 166 (rapporteur), 167 (Greens), 168 (rapporteur), 169 (Greens), 170 (rapporteur), 171 (rapporteur), 172 (Greens)
Falls: 162 (ECR),

The *persons targeted* ~~targets~~

-14 (new). 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, 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 (44). 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^{7a}. 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. (42, 43)

14. 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 2019³⁴, ~~Those targets were~~ namely *the* opposition Senator, Krzysztof Brejza, *the* lawyer, Roman Giertych, and *the* prosecutor, Ewa Wrzosek. ~~who were hacked with Pegasus spyware that was obtained by the government in 2017. While the government has some members of the ruling majority have confirmed the purchase of the software from the NSO Group, the government~~ it has not officially acknowledged that any specific persons were targeted. None of the *three* targets ~~mentioned below~~, 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 are holding *public political* office *in relation to this case. (164)*

Footnotes:

³⁴ 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.

14 a (new). Previously, Citizen Lab had detected a number of infections in Poland in late 2017; however, they were not able to identify the victims at that time^{1a}. (165, 166)

Footnote:

^{1a} AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e>, 21 December 2021.

14 b (new). The use of spyware and efforts to control citizens must be seen 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 previously of the 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 (founding an agrarian political party, competing for the same electorate as the governing parties). (169, 170)

14 c (new). 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, the District Court in Warsaw responsible for the registration of new political parties^{1a} has been filled with government-loyal ‘neo-judges’, whose independence could be called into question.

Footnote:

1a Act of 27 June 1997 on Political Parties,

<https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970980604/U/D19970604Lj.pdf>, at Article 11.

COMP 13 (Paragraph 15 to paragraph 15 e (new))

Paragraph 15

Covered: 174 (EPP), 175 (Greens), 176 (rapporteur), 177 (rapporteur), 178 (Greens), 179 (rapporteur), 180 (Greens), 181 (Greens), 182 (rapporteur), 220 (EPP)
Falls: 173 (ECR), 219 (ECR), 221 (EPP)

Senator Krzysztof Brejza

15. Senator Krzysztof Brejza was serving as *the head of the election* campaign leader of the opposition party Civic Platform *during the European and national elections* when he ~~was~~ *became* the victim of hacking with spyware³⁶. There were 33 attacks on Brejza's phone while he was running the Civic *Platform's* campaign *for the parliamentary elections* in 2019, with the attacks beginning on 26 April 2019 and continuing until 23 October 2019, just days after the end of the election cycle³⁷. (174)

Footnote:

36 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.

37 The Guardian, 'More Polish opposition figures found to have been targeted by Pegasus spyware', 17 February 2022.

15 a (new). *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)^{1a} during the 2019 elections in an alleged orchestrated smear campaign^{1b}. This has caused Senator Brejza to call into question the legitimacy of the 2019 election, which was narrowly won by the ruling PiS Party^{1c}.* (175, 176)

Footnotes:

1a Commission 2022 Rule of Law Report, Poland Specific Chapter, 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.

1b AP, <https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab>, 23 December 2021.

1c Financieel Dagblad, <https://fd.nl/politiek/1426857/liberalen-europarlement-eisen-onderzoek-naar-spyware>, 12 January 2022.

15 b (new). *Although the PiS Government admits to obtaining Pegasus, it vehemently denies allegations that it was used for political purposes^{1a}. Kaczynski has neither confirmed nor denied targeting Brejza, but has alleged that the Senator was linked to 'suspected crimes', something Brejza strongly denies^{1b}. 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^{1c}.* (177, 178)

Footnotes:

1a Politico, <https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/>, 7 January 2022.

1b Politico, <https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/>, 7 January 2022.

1c BBC, <https://www.bbc.com/news/technology-57881364>, 19 July 2021.

15 c (new). *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 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.*

15 d (new). *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^{1a}. 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. (179, 180)*

Footnote:

1a AP, <https://apnews.com/article/technology-business-software-hacking-spyware-8cc528ba7d46a61b378adf1ede9dd00f>, 10 January 2022.

15 e (new). *Ryszard Brejza himself received 10 text messages between July and August 2019 which Amnesty International's security lab deemed suspicious and matched the hallmarks of Pegasus^{1a}. The former assistant of Senator Brejza, Magdalena Losko, also received four suspicious text messages in April 2019 while running Senator Brejza's European Parliament Campaign, which, according to Amnesty International forensic examiners, were technically consistent with the NSO Group's spyware Pegasus^{1b}. (181, 182)*

Footnotes:

1a 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.

1b The Guardian, 'More Polish opposition figures found to have been targeted by Pegasus spyware', 17 February 2022.

COMP 14 (Paragraph 16 to paragraph 16 b (new))

Paragraph 16

Covered: 185 (EPP), 186 (rapporteur), 187 (Greens), 188 (Greens), 189 (rapporteur)
Falls: 183 (ECR), 184 (ID)

Roman Giertych

16. Roman Giertych was targeted with the Pegasus spyware during the *last concluding* 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 the majority of which took* place just before the 13 October 2019 election date. At that time, he was serving as the lawyer of the opposition leader *of Civic Platform and former Prime Minister* Donald Tusk. During that period, Giertych was also representing Radek Sikorski, the former Foreign Minister and currently MEP with the European People's Party (EPP). Sikorski was taking a case to investigate the involvement of Kaczynski and his allies in illegal wiretapping that resulted in the recording and publication of the minister's conversations³⁸.

Footnote:

38 AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e>, 21 December 2021.

16 a (new). *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 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^{1a}. (186, 187)*

Footnote:

1a AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e>, 21 December 2021.

16 b (new). *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 Kaczyński, 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 Kaczyński who then cancelled the project. Birgfellner alleges that he was never paid for his services and so engaged Giertych^{1a}. 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'^{1b}. (188, 189)*

Footnotes:

1a 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.

1b TVP Info, <https://www.tvp.info/57607147/zaryn-ws-senatora-brejzy-falszywe-sa-sugestie-ze-sluzby-nielegalnie-wykorzystuja-kontrolę-operacyjną-do-gry-politycznej>, 23 December 2021.

COMP 15 (Paragraph 17 to paragraph 17 b (new))

Paragraph 17

Covered: 191 (EPP), 193 (rapporteur), 194 (Greens), 195 (Rapporteur)
Falls: 190 (ECR), 192 (ID),

Ewa Wrzosek

17. Prosecutor Ewa Wrzosek was the victim of hacking with the Pegasus spyware as many as six times between the 24th June and the 19th August 2020³⁹. Wrzosek is a member of Lex Super Omnia, *an association which is a group comprised of prosecutors working for the independence of the Office of the Prosecutor*. She was investigating the *decision to hold the 2020 safety of conducting presidential elections in Poland* in the midst of the global COVID-19 pandemic when she was stripped of the case, which was subsequently dropped, ~~and sent away to the city of Srem with 48 hours' notice~~. It is within the growing powers of the PiS Prosecutor-General, Zbigniew Ziobro, *as well as his right-hand man, National Prosecutor Bogdan Świączkowski, to decide elect* not to prosecute certain cases or to remove subordinate prosecutors from *particular cases files*⁴⁰. *Afterwards, prosecutor Wrzosek was sent away, with only 48 hours' notice, to another prosecutor's office in a city several hours away from her home*. It was upon Wrzosek's return to Warsaw that she was targeted with *the Pegasus* spyware. The Polish authorities followed the pattern of declining to confirm or deny their responsibility^{41 42}. (191)

Footnotes:

39 AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e>, 21 December 2021.

40 Commission 2022 Rule of Law Report, Poland Specific Chapter, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, p. 16.

41 AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e>, 21 December 2021.

42 The Guardian, <https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony>, 24 January 2022.

17 a (new). 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 evidence that could be used against her in other cases^{1a}.

Footnote:

1a PEGA Committee meeting, 19 January 2023.

17 b (new). 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^{1a}. 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. (193, 194)

Footnote:

1a PEGA Committee meeting, 19 January 2023.

COMP 16 (Paragraph 18)

Paragraph 18

Covered: 198 (EPP), 199 (EPP), 204 (rapporteur), 205 (Greens),
Falls: 196 (RE), 197 (RE), 200 (ID), 201 (ECR), 202 (Greens), 203 (rapporteur), 206 (Greens),
207 (rapporteur), 208 (Greens), 209 (rapporteur), 210 (Greens), 211 (rapporteur)

Other Possible Targets

Supreme Audit Office

18. *Although not a victim of Pegasus, the NIK – the Supreme Audit Office – which is tasked with safeguarding public spending and with the management of public services, disclosed the invoices for the ‘purchase of special technology means for detecting and preventing crime’ for a total amount of PLN 25 million (199, 198), 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 in Poland has been used predominantly for political purposes^{1a}. (204, 205)*

~~18 The function of NIK, as one of the oldest institutions in Poland, is to safeguard public spending and management of public services. Marian Banās is currently serving as the head of the body⁴³ and has been pushing back against the erosion of the rule of law, and leading the charge for accountability from the PiS government in these cases of hacking, despite being a former ally of the party⁴⁴~~

Footnote:

1a 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.

COMP 17 (Paragraph 19 to paragraph 20)

Paragraph 19

Covered: 212 (ID) 215 (Greens), 216 (rapporteur), 217 (Greens), 218 (rapporteur), 219 (ECR), 220 (EPP), 221 (EPP)

Falls: 213 (ID), 214 (ECR),

PiS Associates

19. ~~It is believed by some~~ **It appears** that Pegasus was used for the ‘preventive tapping’ of leaders and organisers of street protests, responding to the reforms of the Constitutional Court implemented by the PiS Party. However, it is not only opponents of the ruling party that may have fallen victim to Pegasus. **According to sources cited by Wyborcza**, Adam Hofman, former PiS Party spokesperson ~~also alleges that his own colleagues~~ **was** spied upon ~~him~~ in 2018, making him one of the first targets following the purchase of the spyware. Hofman founded R4S, a PR company, after being expelled from the PiS Party^{45 46}. 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.

Footnotes:

45 <https://wyborcza.pl/7,173236,28015977,polish-state-surveilled-nearly-50-targets-with-pegasus-spyware.html?disableRedirects=true>.

46 Rzeczpospolita, <https://www.rp.pl/polityka/art4805251-hofman-usuniety-z-pis-decyzja-w-sprawie-hofmana>, 11 October 2014.

19 a (new). *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^{1a}. Mariusz A. Kaminski was expelled from the PiS Party as a result of being embroiled in a scandal at the same time as Hofman; however Jackiewicz remains a member of the ruling party in spite of his sudden step back from his ministerial role^{1b}. (215, 216)*

Footnotes:

1a <https://wiadomosci.onet.pl/kraj/pegasus-oto-kolejne-osoby-ktore-mialy-byc-inwigilowane-przez-sluzby-pis/yvt6tyu>.

1b <https://nextvame.com/dawid-jackiewicz-is-back-jaroslaw-kaczynski-confirms-the-reports/>.

19 b (new). *A similar smear campaign was also conducted against the former President of the Employers of the Republic of Poland, Andrzej Malinowski, in February 2018 by the ruling party. 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^{1a}. He outlined that messages were taken from his WhatsApp and SMS through 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. (217, 218)*

Footnote:

1a <https://www.senat.gov.pl/prace/komisje-senackie/przebieg,9668,1.html>.

Paragraph 20

Covered: 220 (EPP)

Falls: 223 (ECR)

Connection with Smear Campaigns

~~20. — For weeks on end, Senator Brejza was the target of a smear campaign that made use of material obtained through the use of spyware. It is remarkable that such material was made public via public television. How can it be explained that a public broadcaster gets 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 is also captured by the government party, rather points in the direction of a smear campaign orchestrated by the government parties.~~

COMP 18 (Paragraph 20 a (new) to paragraph 20 b (new))

Covered: 31 (EPP), 33 (EPP), 35 (EPP), 37 (EPP), 66 (RE), 67 (rapporteur), 68 (Greens), 69 (RE), 76 (RE)

Falls: 32 (ECR), 34 (ID), 36 (ECR)

Conclusion

20 a (new). The abuse of Pegasus in Poland *has to be seen in the full context of the rule of law crisis in the country that started in 2015 when the government, led by the Law and Justice Party (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. (31, 66) 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. (31, 33)*

20 b (new). 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 (35, 37). ~~All safeguards have been eliminated removed, giving the government parties full control while victims have nowhere to turn no redress mechanism at their disposal. 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.~~

Compromises on Hungary

COMP 19 (Paragraph 21 to paragraph 21 b (new))

Covered: 222 (rapporteur), 225 (S&D)

I.B. Hungary

21. Hungary was one of the first countries to become embroiled in the European spyware scandal. In 2021, it was revealed by the Pegasus Project ~~that a number of Hungarian phone numbers were listed among the 50.000 identified as potentially hacked by the NSO product. It has since been~~ and confirmed by Amnesty International⁴⁷ 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. (222, 225)

21 a (new). *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.*

21 b (new). *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.*

COMP 20 (Paragraph -22 a (new) to paragraph 22 a (new))

Covered: 231 (RE), 232 (S&D),
Falls: 228 (ECR), 229 (ID), 230 (EPP)

Purchase of Pegasus

-22 a (new). *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^{1a}. However, the procedure was secret and the requests for approval did not specify the specific brand and type of technology^{1b}.*

Footnotes:

1a 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](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-kemsoftver-beszerzesenek-rejtelyei/>.

^{1b} PEGA mission to Hungary, meeting with members of the National Security Committee of the Hungarian Parliament, 20-21 February 2023.

22. The Hungarian Ministry of the Interior bought Pegasus *for EUR 6 million indirectly through Communication Technologies Ltd* from the NSO Group's company in Luxembourg (231) in 2017, shortly after Prime Minister Viktor Orbán met with his Polish counterpart Mateusz Morawiecki and Israeli Prime Minister Benjamin Netanyahu^{49 50}. 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 government⁵¹ – Kósa still insisted, however, that the spyware has never been used against Hungarian citizens⁵².

Footnotes:

49 Financieele Dagblad, *De wereld deze week: het beste uit de internationale pers*. 7 January 2022.

50 The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

51 DW, *Hungary admits to using NSO Group's Pegasus spyware*, 4 November 2021.

52 DW, *Hungary admits to using NSO Group's Pegasus spyware*, 4 November 2021.

22 a (new). *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.*

COMP 21 (Paragraph 23 to paragraph 23 b (new))

Covered: 238 (S&D), 240 (rapporteur), 241 (Greens), 244 (Greens), 245 (rapporteur), 246 (Greens), 247 (rapporteur), 282 (Greens), 283 (rapporteur)

Falls: 237 (ECR), 239 (ID)

Legal framework

23. *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^{1a}. 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 (246, 247)^{1b}.*

Requests for the authorisation of surveillance do not mention the type of technology that will be used^{1c}.

Footnotes:

1a European Union Agency for Fundamental Rights (FRA), 'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary', 26 September 2014.

1b FRA, 'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary', legal update, 23 October 2017

1c PEGA mission to Hungary, 20-21 February 2023.

~~The legal instruments governing spyware in Hungary are some of the weakest such provisions in Europe⁵³⁻⁵⁴. The system exists in blatant violation of European requirements and standards set for the surveillance of citizens by the ECHR and the rulings of the ECtHR⁵⁵ despite the government's insistence that they have acted legally in all instances and are completely compliant with the law⁵⁶⁻⁵⁷. The Act CXXV of 1995 on National Security Services (hereinafter the Act) is currently governing the use of spyware in Hungary⁵⁸ and it is much more of a tool for control and power for the government than a shield for citizens' rights and privacy. Not only does it omit a requirement for the notification of surveillance subjects, it specifically stipulates that targets must not be informed by the authorising party that they are being spied upon.⁵⁹ The requirement to notify victims was unequivocally established in the case of *Klass and others v. Germany*⁶⁰ in the ECtHR and the Hungarian government have failed to implement this ruling in the same manner as Poland and many other countries within the EU.~~

23 a (new). 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.

23 b (new). In a landmark case (*Szabó and Vissy v. Hungary*^{1a}), 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^{1b}. The requirement to notify victims was unequivocally established in the case of *Klass and others v. Germany*^{1c} by the ECtHR. Moreover, there are no effective avenues for remedy and redress in the event of abuse and no proper oversight (AM 238, AM 240, AM 241, AM 282, AM 283). The Hungarian Government has so far failed to implement either ruling.

Footnotes:

1a *Szabó and Vissy v. Hungary*, application no 37138/14, judgment of 12 January 2016, [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-160020%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}).

1b Act CXXV of 1995 on National Security Services,

http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf.

1c *Klass and others v. Germany*, 6 September 1978, paragraph 50, Series A, no. 28.

COMP 22 (Paragraph 24 to paragraph 24 e (new))

Covered: 233 (Greens), 234 (rapporteur), 249 (rapporteur), 250 (Greens), 251 (Greens), 252 (rapporteur), 253 (rapporteur), 254 (Greens), 255 (Greens), 256 (rapporteur), 257 (Greens), 258 (rapporteur)
Falls: 248 (ECR)

Ex ante scrutiny

24. ***According to the National Security Act*** ~~Per the 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 ~~the majority of~~ instances, and on the judge designated by the President of the ~~Budapest Capital Regional~~ **Metropolitan Court of Budapest** in some specific cases^{61 62}. No appeal can be ~~made~~ **lodged** against these decisions and there is virtually no oversight of the process^{63 64}.

Footnotes:

61 Act CXXV of 1995 on National Security Services,

http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Sections 56-58.

62 Study – Europe’s PegasusGate: Countering spyware abuse, European Parliament. Directorate-General for Parliamentary Research Services, 6 July 2022,

[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU\(2022\)729397_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf), at p. 20.

63 Act CXXV of 1995 on National Security Services,

http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, at Sections 57 and 58.

64 Commission 2022 Rule of Law Report Country Chapter on the rule of law situation in Hungary,

https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, at p. 26.

24 a (new). 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^{1a}. This was confirmed by Repassy himself in a response he authored to written questions on the issue^{1b}. 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^{1c}. 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^{1d}. (249, 250)

Footnotes:

1a <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](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf), July 2022, at p. 20.

1b <https://telex.hu/belfold/2022/01/27/varga-judithoz-kerulhetett-vissza-a-titkos-megfigyelesek-engedelyezese>.

1c <https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korruptcios-ugye>; <https://hungarytoday.hu/444-key-figure-in-volner-corruption-case-gyorgy-schadl-judge-fired-judiciary-obh/>.

1d <https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korruptcios-ugye>.

24 b (new). While Interior Minister Sándor Pintér insists that this authorisation procedure through the minister or the courts is always followed without exception^{1a}, 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^{1b}. (251, 252)

Footnotes:

1a AP, <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>, 4 November 2021.

1b Act CXXV of 1995 on National Security Services,

http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, at Section 59.

24 c (new). The legal limit of a maximum of 90 days for surveillance imposed by the Act can be extended for a further 90 days upon a simple request from a director-general to the permitting officer^{1a}, which is only provided for to give the appearance of a legal safeguard. (255, 256)

Footnote:

1a Act CXXV of 1995 on National Security Services,

http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, at Section 58.

24 d (new). 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^{1a}. (233, 234). 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^{1b}. According to Péterfalvi, the NAIH investigation did not uncover any illegal activity or anything inconsistent with the terms of sale of the NSO Group^{1c}.

Footnotes:

1a HVG, https://hvg.hu/itthon/20111117_Peterfalvi_palyaja_adatvedelem, 21 November 2011.

1b PEGA mission to Hungary, 20 February 2023.

1c Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 February 2022.

24 e (new). The head of the NAIH is appointed by the Prime Minister, hence their independence can be called into question^{1a}. The ECtHR ruled on the matter in September 2022 in a case of Hüttl v. Hungary^{1b} 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^{1c}. 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^{1d}. 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^{1e}. (238, 257, 258)

Footnotes:

1a <https://hclu.hu/en/pegasus-whats-new>.

1b [https://hudoc.echr.coe.int/fre#{%22tabview%22:\[%22document%22\],\[%22itemid%22:\[%22001-219501%22\]\]}](https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],[%22itemid%22:[%22001-219501%22]]}).

1c <https://tasz.hu/cikkek/valoszinusithetoen-lehallgattak-pert-nyert-strasbourgban-a-tasz-ugyvedje>:
<https://hudoc.echr.coe.int/fre?i=001-219501>.

1d <https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere>.

1e <https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere>.

COMP 23 (Paragraph 25 to paragraph 25 d (new))

Covered: 235 (Greens), 236 (rapporteur), 260 (RE), 261 (S&D), 263 (Greens), 264 (rapporteur), 265 (Greens), 266 (rapporteur), 267 (rapporteur), 268 (Greens), 269 (Greens), 270 (rapporteur)

Falls: 259 (ECR), 262 (ID)

Ex post scrutiny

25. In November 2021, ~~at~~ **on** the insistence of the opposition, ***the National Security Committee and Committee on Defence and Security*** ~~two committees~~ in the ~~Senate~~ ***National Assembly*** conducted hearings into the use of spyware in Hungary and the alleged politically motivated targeting of citizens by the government in particular. ~~It was subsequently reported that the government~~ ***The government party held 4 out of 6 seats in the National Security Committee and prevented any meaningful and democratic scrutiny of the use of Pegasus. The*** representatives ***of the government party*** insisted that all surveillance ~~was~~ ***had been*** authorised through ***the*** appropriate channels, but refused to comment on whether or not journalists or politicians ~~were~~ ***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***^{1a}. It is not possible to know exactly what was said, however, as the ruling party have classified the minutes of the meeting until ~~the year~~ 2050 (235, 236)^{1b}.

Footnotes:

1a PEGA mission to Hungary, meeting with members of the National Security Committee of the Hungarian Parliament, 20 February 2023.

1b AP,

<https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>, 4 November 2021.

25 a (new). *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^{1a}. The resulting report was published on 31 January 2022 and concluded that the use of Pegasus was strictly for reasons of national security.*

Footnote:

1a 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.

25 b (new). *Similarly, the Hungarian prosecution service closed its investigation into the targeting on 15 June 2022, concluding that no unauthorised surveillance had taken place. (265, 266)*

25 c (new). *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. (267, 268)*

25 d (new). *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^{1a}. (269, 270)*

Footnote:

1a 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.

COMP 24 (Paragraph 26 to paragraph 26 d (new))

Covered: 273 (S&D), 274 (rapporteur), 275 (Greens), 276 (rapporteur), 277 (Greens), 278 (Greens), 279 (Greens), 280 (Greens), 281 (rapporteur),
Falls: 271 (ECR), 272 (ID)

Redress

26. When the Pegasus scandal erupted in Hungary, ~~it became clear that~~ journalists were one of the groups most targeted by the government, ~~though it refuses to either confirm or deny this.~~ 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 (273) proceedings in Hungary against both the State and the NAIH.** The Hungarian Civil Liberties Union (HCLU) ~~will~~ 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 Group**⁶⁵.

Footnote:

65 The Guardian, <https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state>, 28 January 2022.

26 a (new). *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.* (274, 275)

26 b (new). *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.* (276, 277)

26 c (new). *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^{1a}. 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^{1b}.* (278, 279)

Footnotes:

1a <https://hclu.hu/en/pegasus-case-hungarian-procedures>.

1b <https://hclu.hu/en/pegasus-whats-new>.

26 d (new). *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 victims 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^{1a}. This creates another pretext for the Hungarian authorities to once again fall back on national security reasons^{1b}. So far, the Constitution Protection Office has rejected 270 freedom of information requests submitted by the HCLU between 2018 and May 2022^{1c}. (280, 281)*

Footnotes:

1a <https://hclu.hu/en/pegasus-case-hungarian-procedures>.

1b <https://hclu.hu/en/pegasus-whats-new>.

1c <https://hclu.hu/en/pegasus-whats-new>.

COMP 25 (Paragraph 27 to paragraph 27 c (new))

Covered: 242 (rapporteur), 243 (Greens), 286 (S&D), 287 (Greens), 288 (rapporteur), 289 (Greens), 290 (rapporteur)

Falls: 284 (ID), 285 (ECR)

Political control

27. ~~The~~ Political control over the use of surveillance in Hungary is complete ~~and total~~. The Orbán-led Fidesz regime has ~~made it so that~~ **created a system in which** they can target lawyers, journalists, political opponents and civil society organisations ~~with ease and without fear of recourse~~. In addition, their control over almost all Hungarian media outlets allows them to ~~continue pushing their own version of the truth, stopping much of the public scrutiny conducted by the media from reaching Hungarian citizen~~.

27 a (new). *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. 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. (287, 288)*

27 b (new). *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 Constitutional Court, the Supreme Court, the Court of Auditors, the prosecution service, the National Bank of Hungary and the National Election Committee^{1a}. 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^{1b}. (289, 290)*

Footnotes:

1a 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.

1b 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.

27 c (new). 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 victims' 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^{1a}. 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^{1b}. Moreover, owing to this purchase, the state will have an access point to the decades-old global messaging system known as SS7^{1c}. 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^{1d}. (242, 243)

Footnotes:

1a Reuters, <https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/>, 22 August 2022.

1b Reuters, <https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/>, 22 August 2022; Volkskrant, Orbán versterkt met overname Vodafone Hongarije grip op telecommunicatie, critici uiten zorgen.

1c The Guardian, <https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands>, 16 December 2020.

1d <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>.

COMP 26 (Paragraph 28)

Covered: 293 (RE)

Falls: 291 (ECR), 292 (ID)

The targets

28. ~~It has been very clear that the government's actions were politically motivated from the moment that the spyware scandal broke in Hungary.~~ It was reported that the phone numbers of over 300 persons were included in the findings of the Pegasus Project⁶⁶. Among ~~those~~ **them** were at least five journalists, ~~ten~~ **10** lawyers, **the mayor of Gödöllő, who is a member of and an opposition party politician, an employee of the opposition party,** as well as activists and high-profile business owners⁶⁷. **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 ~~hacking of those phones took place,~~ 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.***

Footnotes:

66 The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021.

67 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 The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021.

COMP 27 (Paragraph 29 to paragraph 29 c (new))

Covered: 297 (Greens), 298 (rapporteur), 299 (Greens), 300 (rapporteur)

Falls: 294 (ECR), 295 (ECR), 296 (ID)

Szabolcs Panyi

29. The hacking of ~~the phone of~~ journalist and editor Szabolcs Panyi's **phone** occurred ~~through~~ **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 a valuable by-catch for the government.

29 a (new). *Amnesty International confirmed that Panyi's phone had been consistently hacked in 2019 over a period of seven months^{1a}. 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^{1b}. 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^{1c}. That equates to over half of Panyi's requests resulting in being targeted within that seven-month period^{1d}. (297, 298)

Footnotes:

1a The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

1b The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

1c The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

1d The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

29 b (new). *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 political activist, as well as accusing him of Orbánophobia and Hungarophobia^{1a}. 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. (299, 300)*

Footnote:

1a The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

29 c (new) *Following an investigation by Panyi into the Hungarian broker company Communication Technologies Ltd, through which Pegasus was purchased, the company sued him^{1a}.*

Footnote

1a PEGA mission to Budapest, 20-21 February 2023.

COMP 28 (Paragraph 30 to paragraph 30 d (new))

Covered: 304 (Greens), 305 (rapporteur), 306 (rapporteur), 307 (Greens), 308 (Greens), 309 (rapporteur)

Falls: 301 (ECR), 302 (ECR), 303 (ID)

Zoltán Varga

30. As CEO and Chairman 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 party³⁰.

Footnote:

30 <https://www.mapmf.org/alert/25319>.

30 a (new). *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^{1a}. 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^{1b}. 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^{1c}. (304, 305)*

Footnotes:

1a 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.

1b The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

1c The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021.

1d PEGA mission to Budapest, 20-21 February 2023.

30 b (new). *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^{1a}. 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^{1b}. 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 'dangerous'^{1c}. (306, 307)*

Footnotes:

1a The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

1b The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

1c The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021.

30 c (new). *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. (308, 309)*

30 d (new). *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^{1d}.*

Footnote:

1d PEGA mission to Budapest, 20-21 February 2023.

COMP 29 (Paragraph 31 to paragraph 31 b (new))

Covered: 313 (S&D), 314 (Greens), 315 (rapporteur), 316 (Greens), 317 (rapporteur)

Falls: 310 (ECR), 311 (ECR), 312 (ID)

Adrien Beauduin

31. Adrien Beauduin appeared on the radar of the Orbán regime in 2018, while completing a PhD in gender studies at the Central European University (CEU). 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 studies⁶⁸. After attending a protest in Budapest, Beauduin was arrested in what is seen as a highly politically motivated move, and faced charges for assaulting a police officer, which he vehemently denies⁶⁹. 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 case⁷⁰. ***In 2020, the criminal proceedings against Adrien Beauduin, who was represented by the HCLU in the case, were terminated (313).***

Footnotes:

68 The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

69 The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

70 The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

31 a (new). Government representatives publically condemned the so-called pro-immigration Soros network for orchestrating ‘violent demonstrations in Budapest’^{1a}. Subsequently, traces of Pegasus were found on Beauduin’s phone, but it was not possible to confirm whether there had been a successful infection. (314, 315)

Footnote:

1a The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

31 b (new). 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^{1a}. (316, 317)

Footnote:

1a <https://tasz.hu/a/files/220816-Complaint-unlawful-surveillance.pdf>.

COMP 30 (Paragraph 32 to paragraph 32 c (new))

Covered: 321 (RE), 322 (RE), 331 (RE)

Falls: 318 (ECR), 319 (ECR), 320 (ID)

Ilona Patócs

32. 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 case⁷¹. However, owing to the type of mobile device she was using, it was not possible to confirm whether the hack was fully successful or ~~when~~ exactly **when** it occurred. Her client, István Hatvani, had already served seven years for an assassination, which Patócs claims was a ‘politically motivated’ conviction⁷². 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 Bánáti⁷³ **(331)**. This targeting in particular shows a clear disregard **by** ~~from~~ the government for the privilege that exists between lawyers and their clients.

Footnotes:

71 Direkt36, <https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/>, 31 March 2022.

72 Direkt36, <https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/>, 31 March 2022.

73 Direkt36, <https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/>, 31 March 2022.

György Gémesi

32 a (new). *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. (321)*

Brigitta Csikász

32 b (new). *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; (322)*

32 c (new) *President of the Hungarian Bar Association, János Bánáti, criminal defence lawyer and several other lawyers were also targeted with Pegasus (331).*

COMP 31 (Paragraph 33 to paragraph 33 a (new))

Covered: 323 (RE), 327 (RE), 328 (RE), 329 (rapporteur), 330 (Greens),
Falls: 324 (ECR), 325 (ECR), 326 (ID)

Other targets

33. People inside the ruling party's circle have also been targeted with spyware. ~~It was reported by t~~The independent Hungarian outlet Direkt36 **reported** in December 2021 that ***the head of the protection service and the personal*** a bodyguard of János Áder, the President and close ally of Orbán, ***had been*** was hacked with Pegasus spyware. Direkt36 journalist and victim of spyware Szabolcs Panyi has reported that this kind of spying is mainly as a result of the growing paranoia of the Hungarian Prime Minister. (327) ***Cecília Szilas, former ambassador of Hungary to China, was targeted with Pegasus shortly before becoming senior adviser to Viktor Orbán. (328) 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 (323).***

33 a (new). Furthermore, both the son and lawyer of one of Orbán's oldest friends, Lajos Simicska, were hacked with Pegasus^{1a}. 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^{1b}. 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^{1c}. 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^{1d}. 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. (329, 330).

Footnotes:

1a The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021.

1b The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021

1c The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021.

1d The Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/>, 19 July 2021.

COMP 32 (Paragraph 34 to paragraph 34 b (new))

Covered: 334 (S&D), 335 (Greens), 336 (rapporteur), 337 (rapporteur), 338 (Greens)
Falls: 332 (ECR), 333 (ID)

Spyware companies

34. The Hungarian Government has not only purchased and utilised Pegasus spyware against its people, but ~~it~~ **also** been playing host to other companies in the intelligence market ~~also~~ **such as Black Cube and Cytrox (334)**. Black Cube is an Israeli private intelligence agency comprised of former employees of Mossad, the Israeli military and Israeli intelligence services⁷⁴. Their own company website dubs them as a 'creative intelligence service' finding 'tailored solutions to complex business and litigation challenges'⁷⁵. Black Cube have been involved in a number of public hacking controversies, including in the US and Romania⁷⁶.

Critically, **links have** it has also been uncovered that they are 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 at in at least one situation in Cyprus.

Footnotes:

74 The New Yorker, <https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators>, 7 October 2019.

75 <https://www.blackcube.com/>.

76 The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

34 a (new). *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^{1a}. Those targeted included lawyer and member of the leading human rights NGO Hungarian Helsinki Committee, Marta Pardavi^{1b}. 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^{1c}. (335, 336)*

Footnotes:

1a Politico, <https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/>, 6 July 2018.

1b Reuters, <https://www.reuters.com/article/meta-facebook-cyber-idCNL1N2T12MC>, 16 December 2021.

1c Politico, <https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/>, 6 July 2018.

34 b (new). *An additional connection with Hungary is Cytox Holdings Zrt., which is registered to an address in Budapest. Cytox, 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. (337, 338)*

COMP 33 (Paragraph 34 c (new) to paragraph 34 d (new))

Cover: 226 (Greens), 227 (rapporteur), 286 (S&D)

Falls: 223 (ECR), 224 (ID)

Conclusion

34 c (new). *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^{1a}. 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 (286).*

Footnote:

1a The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

34 d (new). 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^{1a 1b}. 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^{1c} despite the government's insistence that it has acted legally in all instances and complies fully with the law^{1d 1e}. Although the government consistently falls back on reasons of 'national security'^{1f}, its claims that the victims are a threat to national security are not credible. (226, 227)

Footnotes:

1a The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

1b DW, 'Pegasus scandal: In Hungary, journalists sue state over spyware', 29 January 2022.

1c 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.

1d AP, <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>, 4 November 2021.

1e Euractiv, *Hungary employed Pegasus spyware in hundreds of cases, says government agency*, 1 February 2022.

1f Euractiv, *Hungary employed Pegasus spyware in hundreds of cases, says government agency*, 1 February 2022.

Compromises on Greece

COMP 34 (Paragraph -35 a (new) to -35 b (new))

Covered: AM 377 (EPP), AM 382 (EPP)

Fall: AM 381 (EPP)

I.C. Greece

-35 a (new). *The Committee visited Greece in November 2022 as part of a joint mission Greece/Cyprus. Members met with 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 with investigative journalists, Members of the Hellenic Parliament and the President of the Data protection Authority ADAE, NGOS and Human rights defenders (AM 377).*

-35 b (new). *The visit brought to light that more 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 installed, reforms should improve transparency and ensure appropriate judicial oversight over the use of surveillance (AM 382). The visit also confirmed that clear rules are needed for limiting the use of national security as grounds for surveillance, ensuring proper judicial oversight, and guaranteeing a healthy, pluralist media environment.*

COMP 35 (Paragraph 35 to Paragraph 37)

Covered: AM 343 (Rapporteur), AM 344 (S&D), AM 345 (Left), AM 348 (rapporteur), AM 349 (Greens), AM 351 (Left), AM 352 (Greens), AM 353 (Rapporteur), AM 354 (Left), AM 355 (Greens), AM 356 (Rapporteur)

Fall: AM 339 (EPP), AM 340 (EPP), AM 341 (EPP), AM 342 (ECR), 346 (ID), AM 347 (Left), AM 350 (Εμμανουήλ Φράγκος), AM 366 (Left)

35. Throughout 2022, ~~This year~~ Greece ~~has been~~ **was** shaken by a series of ~~reports~~ **revelations** regarding the ~~evidently politically motivated~~ 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 cell phone with Predator spyware.⁷⁷ The attempted infection with spyware was discovered during a check of Androulakis' phone by the European Parliament IT service⁷⁸. **According to forensic analysis of IT Service** ~~the~~ **the** hacking attempts happened while 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 phone with Predator. **His infection was confirmed by CitizenLab.** In September, ~~it was revealed that~~ former Minister of Infrastructure and lawmaker for the Syriza party, Christos Spirtzis,⁷⁹ ~~had~~ **also claimed to have** been targeted with **the Predator** spyware (AM 344). **Although his mobile phone was not officially checked, Spirtzis did share the links he received with two technicians who verbally confirmed that he**

had been targeted^{79a}. Furthermore, it was revealed later that month that Greece's National Intelligence Service (EYP) had allegedly targeted two of its own employees with spyware⁸⁰. On 5 and 6 November, the Greek media revealed a list of 33 targets of Predator, all of whom were high profile personalities⁸¹. The list, ***neither confirmed nor denied by the government nor by those surveilled (345), ~~if confirmed~~*** reads like a stunning who is who of ***includes names of people working in*** politics, business and media in Greece. ~~The impact of this large-scale political use of spyware is infinitely bigger than just the~~ ***The impact of the alleged surveillance of*** people that appear on the list ***could be more extensive***, as all their respective contacts and connections ~~are~~ ***could be*** indirectly "caught" indirectly in the spying operation as well, including their contacts in EU bodies. The high prevalence of spyware was ***reportedly*** already visible in the 2021 Meta report, which mentioned 310 fake websites links related to the Cytox spyware company in its annex, 42 of which were set up to mislead targets in Greece alone.^{82 83} ***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 cross-referenced with the one published by the 2021 Meta report***^{83a} (343). ***On 28 February 2023, the President of the Hellenic Data Protection Authority (APDPX) confirmed that 300 text messages related to Predator spyware have been sent to approximately 100 devices. The President of the The Hellenic Authority for Communication Security and Privacy (ADAE) additionally stated that the ADAE acted upon several complaints and found two cases of Predator and one bank account number of a person behind the false text messages. The ADAE investigation into new complaints is ongoing***^{83b}.

Footnotes:

77 Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.

78 Tagesspiegel. Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.

79 Reuters. One more Greek lawmaker files complaint over attempted phone hacking.

79a. <https://insidestory.gr/article/predator-perissoteroi-apo-20-oi-stohoi-toy-stin-ellada-symfona-me-tin-arhi-prostasias>

80 Efsyn. Targeting the disliked.

81 <https://www.documentonews.gr/article/poiouys-kai-giati-akoyge-to-systima-mitsotaki/>

82 Meta. Threat Report on the Surveillance-for-Hire Industry.

83 InsideStory. Who was tracking the mobile phone of journalist Thanasis Koukakis?

83a Documento 27 November 2022.

83b. PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.

35 a (new). In August 2022, the Greek government conceded that EYP had indeed been monitoring Androulakis and Koukakis, but it denied that it 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^{1a}. ***To date, the official reasons for the surveillance have not been disclosed (348, 349).***

Footnote:

1a Solomon. Solomon's reporter Stavros Malichoudis 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?

35 b (new). On 8 August 2022, Prime Minister Mitsotakis issued a video message stating ambiguously that the surveillance of Androulakis was "legal" but "politically

unacceptable". He made no reference to the surveillance of Koukakis, nor the alleged other cases. He also stated that he had not been aware of the surveillance, but had he known, he would not have allowed it^{1a}. According to the official statement from the Government spokesman Yiannis Oikonomou, as soon as the Prime Minister became aware of Androulakis's "legal interception", Minister of State Giorgos Gerapetritis sought to fully inform him Androulakis in private about the reasons behind his surveillance.^{1b} Androulakis denied to be informed, stating that such a private briefing would be illegal and that the only lawful course was through the Parliament. Later on, while testifying before the Parliament, Minister Gerapetritis 'declared that he was never aware of the reasons, appealing to top secret secrecy of any relevant information (354). The EYP is under the direct control of Prime Minister Kyriakos Mitsotakis following a legislative amendment, passed soon after his party Néa Dimokratía came to power in 2019^{1c}(353, 352, 351).

Footnotes:

1a Reuters. Greek PM says he was unaware of phone tapping of opposition party leader

1b LIFO: Androulakis denied information in private upon his surveillance <https://www.lifo.gr/now/politics/o-androulakis-arnithike-idiotiki-enimerosi-apo-ton-gerapetriti-kai-zita-na-toy>

1c Euractiv. Another Greek opposition lawmaker victim of Predator.

35 c (new). After the revelations, Grigoris Dimitriadis, the government's General Secretary responsible for the cooperation between the Greek government and the EYP, and EYP Chief Panagiotis Kontoleon, resigned^{1a}.(355, 356)

Footnote:

1a POLITICO. PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal

~~36. The revelations about the use of spyware and EYP surveillance of journalists tell a very disturbing story of an intricate and opaque network of relations, political and business interests, favours and nepotism, and political influence. It is easy to get lost in the maze. However, a few patterns emerge. A political majority is being used for the advancement of particular interests rather than the general interest, notably by the appointment of associates and loyalists in key positions such as the EYP, EAD and Krikel. Whereas spyware, possibly combined with legal interception, is used as a tool for political power and control in the hands of the highest political leadership of the country. 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 and there is no whistleblowers protection.~~

~~37. 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 integral authoritarian strategy, but rather a tool used on an ad hoc basis for political and financial gains. However, it equally erodes democracy and the rule of law, and gives ample room to corruption, whereas these turbulent times call for reliable and responsible leadership.~~

COMP 36 (Paragraph -38 a (new) to Paragraph 38)

Purchase

Covered: AM 358 (Greens), AM 383 (Rapporteur), AM 385 (EPP)

Fall: AM 384 (ID)

-38 a (new) At the end of 2019, Secretary General Dimitriadis was in contact with NSO Group for the purchase of the Pegasus spyware. In January 2020, an official proposal submitted by NSO Group concerned a government-to-government agreement of 50 million euros. After the signing of the agreement, the individual would withdraw and the EYP would take over. The EYP would cooperate with the Mossad for the installation of the system. The proposal was eventually called off^{1a} (383).

Footnote:

1a <https://insidestory.gr/article/greek-state-and-spyware-vendor-intellexa-they-are-acquainted-after-all>

38. Both EYP and the government categorically deny that Predator has ever been purchased or used by the Greek authorities^{1a}. (358). ~~The government denies the purchase of Predator spyware⁸⁴. However, 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 phones of Koukakis and Androulakis. That would be a crime under Greek law and one would expect the Greek authorities to immediately and vigorously investigate such a serious case. However, so far there is no police investigation, only prosecutorial inquiries following complaints. No physical evidence has been seized(385).~~The hypothesis of private actors behind the Predator attacks is moreover highly implausible, as it would not explain the choice of targets.

Footnote:

1a. EPRS. Greece's Predatorgate. The latest chapter in Europe's spyware scandal?

COMP 37 (Paragraph 39)

Covered: AM 386 (S&D), AM 393 (S&D),

Fall: AM 390 (EPP), AM 391 (ID), AM 392 (ECR), AM 394 (Rapporteur), AM 395 (Left)

4039. 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 phones of Koukakis and Androulakis. That would be a crime under Greek law, which would have to be investigated. (385).The hypothesis of private actors 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 for the extensive relations between Intellexa, the company owning Predator spyware and the Greek State (AM 386). On 16 January 2023, the Hellenic Data Protection Authority fined Intellexa 50.000 euros for failing to cooperate and refusing to hand over***

information about its clientele, as part of its investigation launched in July 2020 following Androulakis' complaint. The investigation is still ongoing^{1a} (393).

Footnote:

1a <https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-stin-intellexa-ae-gia-mi-synergasia-me-tin-arhi>

COMP 38 (Paragraph 40)

Covered:

Fall: AM 387 (ID), AM 388 (EPP), AM 389 (Left)

3940. Another One possibility is that Predator was acquired through Ketyak, ~~a special entity~~ **Centre for Technological Support, Development and Innovation** set up by former **Director-General of the EYP** ~~boss~~ Kontoleon. It operates ~~at a distance~~ **independently** from the EYP^{1a} **and participates in projects surrounding research, innovation and technology development^{1b}.**

Footnotes:

1a. <https://www.tovima.gr/print/politics/to-trigono-lfpou-egkatestise-lfto-predator-crstin-ypiresia-crpliroforion-cr kai-i-lista-crton-xeiriston-tou/>

1b. <https://www.nis.gr/en/ketyak>

COMP 39 (Paragraph 41 to Paragraph 41 d (new))

Grigoris Dimitriadis

Covered: AM 398 (S&D), AM 399 (Left), AM 400 (Greens), AM 401 (Rapporteur), AM 402 (Greens), AM 403 (Rapporteur), AM 404 (Greens), AM 405 (Rapporteur), AM 406 (Rapporteur), AM 407 (Greens),

Fall: AM 396 (ECR), AM 397 (ECR)

41. Dimitriadis is the nephew of Prime Minister Mitsotakis, and until August 2022 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 EYP had wiretapped the phone of Androulakis. At the start, 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 Androulakis and other political persons^{1a} (398).**

Footnote:

1a <https://www.iefimerida.gr/politiki/paraitisi-dimitriadi-klima-toxikotitas-ohi-predator?amp;https://primeminister.gr/2022/08/08/29961;>

41 a (new). The former head of the EYP, Panagiotis Kontoleon, admitted to the Greek Parliamentary Inquiry Committee his "social relationship" with Dimitriadis. Kontoleon was appointed by the Mitsotakis government, but some provisions of the law had to be adapted so as to enable his appointment^{1a}. (400, 401, 399).

Footnote:

1a *leidiseis. SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up*

41 b (new). *Dimitriadis is also closely connected in several ways to Felix Bitzios and Giannis Lavranos. The three men are personally acquainted. Dimitriadis and Lavranos are best men ("Koumbaroi")^{1a} and Dimitriadis is the godfather of Lavranos' second child^{1b}. Dimitriadis was also indirectly connected to Bitzios through business transactions with Bitzios' brother^{1c}. (402, 403, 399).*

Footnotes:

1a TVXS. Giannis Lavranos: The koumbarias with Tsouvala and Dimitriadis

1b Ieidiseis. SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up.

1c ReportersUnited. The Great Nephew and Big Brother.

41 c (new). *This puts him at the heart of a network connecting him professionally as well as personally to key persons at Intellexa, Krikel and EYP (404, 405, 399).*

41 d (new). *Dimitriadis is reportedly also acquainted with Adreas Loverdos, candidate for the PASOK-KINAL leadership in 2021. (406, 407, 399).*

COMP 40 (Paragraph 42 to Paragraph 42 a (new))

Felix Bitzios

Covered: AM 411 (Greens), AM 412 (Rapporteur), AM 414 (Left)

Fall: AM 408 (ECR), AM 409 (ECR), AM 410 (EPP),

42. Business man Felix Bitzios had been implicated in the huge Bank of Piraeus violation of capital controls scandal. Pending the investigations, Bitzios' assets had been frozen⁸⁵. 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 months⁸⁶. Thanks to the amendment of the Mitsotakis government, the assets of Bitzios could be released.

Footnotes:

85 Lexocology. Cyprus court offers directions to bank on ambit of freezing injunction.

86 Financial Times. Greek law change viewed as backtracking on money laundering.

42 a (new). *Bitzios is connected with Cyprus through his company Santinomo, registered on Cyprus, and his connection with Tal Dilian. It seems that Bitzios has been instrumental in the transfer of Intellexa to Greece^{1a}. (411, 412, 414).*

Footnote:

1a Inside Story. Predatorgate: The second shareholder of Intellexa SA.

COMP 41 (Paragraph 43)

Covered:

Fall: AM 413 (ECR)

43. 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 Intellexa⁸⁷. ***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.*** ~~What is remarkable is not just the date of the registration of the transfer—just days after the revelations of the Androulakis hack—but the fact that the transfer supposedly took place on 18 December 2020, over 19 months earlier.~~ Bitzios thus retroactively distanced himself from his 1/3 Intellexa ownership. Nevertheless, Bitzios had been connected to Intellexa from March 2020 to June 2021 as a deputy administrator^{87a}.

Footnote:

87 *Inside Story. Predatorgate: The second shareholder of Intellexa SA*

87a <https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae>

COMP 42 (Paragraph 44)

Giannis Lavranos

Covered:

Fall: AM 415 (ECR), AM 416 (ECR), AM 417 (Left)

44. Giannis Lavranos had been charged with tax evasion and journalist Koukakis had been reporting about Lavranos' case.

COMP 43 (Paragraph 45 to Paragraph 45 c (new))

Intellexa

Covered: AM 357 (Rapporteur), AM 359 (Left), AM 361 (Rapporteur), AM 363 (Rapporteur), AM 418 (Left), AM 421 (S&D), AM 422 (Greens), AM 1155 (Greens)

Fall: AM 419 (Rapporteur), AM 420 (Mandl)

45. 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 ex-wife Polish citizen Sara Hamou is a central figure in the intricate network of companies. Tal Dilian also has acquired Maltese citizenship. The ***Greek government*** ~~Ministry of Foreign Affairs in Greece, responsible for the distribution of export permits,~~ declared that ***two*** ~~no~~ export licenses were granted to Intellexa ~~group of companies, of which one authorized the export to Madagascar (418, 419). In addition, the Greek government issued an export license for Predator to Sudan. It has not been confirmed to whom the license had been issued, whether to Intellexa or another entity.~~ ***However,*** Intellexa companies based in Greece ***has*** reportedly ***also*** exported their products to Bangladesh. and at least one Arab country. ~~For a detailed description on Intellexa, see the chapter on the Spyware industry.~~

45 a (new). On November 30, 2022, an investigative report by Lighthouse Reports, in collaboration with the Israeli newspaper Haaretz and the Greek outlet Inside Story, revealed that (AM 1155) 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^{1a} (357). 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 (AM 1155). On 18 February 2023, the European Commission confirmed that they had contacted the national authorities in Greece and Cyprus for clarification on this matter. However, the Commission has not received an answer^{1b}. On 19 April 2023, the Greek alternate foreign affairs minister Miltiadis Varvitsiotis confirmed that the Greek government 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 in Sudan^{1c}.

Footnote:

1a <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>

1b. https://www.europarl.europa.eu/doceo/document/E-9-2022-003990-ASW_EN.html; PEGA Committee Meeting, 28 March 2023.

1c. <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>

45 b (new). In December 2022, the Greek government disclosed that it had provided Intellexa with two export licenses on November 15, 2021 (359, 361). According to spokesperson for the Greek Foreign Ministry Alexandros Papaioannou, one of these licenses authorized the sale of Predator to Madagascar^{1a}. The licence was granted despite the country's poor human rights record^{1b} and potentially being in conflict with the EU dual-use regulation. (361, 422) Secretary General of International Economic Relations Ioannis Smyrlis - who authorized the sale of Predator to Madagascar - handed in his resignation after these revelations came to light^{1c} (361, 421) to take up the post of deputy director-general of the ruling party Nea Dimokratia, which is responsible for the upcoming elections. (421)

Footnotes:

1a 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>

1b 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>

1c The National Herald. Top Greek Official Who Authorized Predator Spyware Sale Resigns.

45 c (new). Besides 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 Interior of Bangladesh, 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^{1a} (363).

Footnote:

1a Haaretz. Israeli Spy Tech Sold to Bangladesh, World's Third-largest Muslim Country, Despite Dismal Human Rights Record.

Krikel

Covered:

Fall: AM 423 (EPP)

46. 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 50% owner of Krikel, through another company called Mexal⁹¹. 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.

Footnote:

91 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: InsideStory. Predatorgate's invisible privates. and tvxs. G.Lavranos behind KRIKEL - How the deception of the Parliament was attempted [Revealing documents].

COMP 45 (Paragraph 47)

Covered: AM 424 (Left), AM 425 (Rapporteur), AM 426 (Greens),

Fall:

47. In 2014, Giannis Lavranos' company Ioniki Techniki was sold to Tetra Communications in London. In this same year, Ioniki Techniki is one of the three companies that donated the Tetra Communications Systems to the Greek Ministry of Citizen Protection⁹². ***In 2014, the Greek government had also shown interest in the Italian spyware brand called RCS Galileo from company Hacking Team, as revealed by Wikileaks, but this software was never acquired^{92a}. (425, 424, 426)*** The donation of Tetra was facilitated by a Florida based company, allowing to bypass regular tender procedures. The donation to the Greek government was accepted in 2017. In 2018, Krikel signed a maintenance and technical support contract of €10.8 million. Krikel administrator Stanislaw Pelczar signed on behalf of Krikel, but it seems that Lavranos was informally involved in the negotiations throughout⁹³. Krikel became an important supplier of the Greek Ministry of Citizen Protection. Since 2018, it signed seven contracts with the Greek government, six of which are secret⁹⁴.

Footnotes:

92 Inside Story. Predatorgate's invisible privates.

92a Inside Story. The timeless interest of the Greek authorities in spyware. <https://insidestory.gr/article/diachroniko-endiaferon-ton-ellinikon-arhon-gia-logismika-kataskopeias>

93 Inside Story. Predatorgate's invisible privates.

94 Inside Story. Predatorgate's invisible privates.

COMP 46 (Paragraph 48)

Covered: AM 427 (EPP),

Fall:

48. Krikel company also became the local representative of Italian company RCS Lab. In June 2021, the EYP **reportedly (427)** purchased a wiretapping system from RCS lab⁹⁵ through Krikel⁹⁶. At that time, Dimitriadis was responsible for the contacts between the government and 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 problem⁹⁷. Other sources however claimed that Kontoleon ordered the destruction of files on 29 July 2022⁹⁸.

Footnotes:

96 TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.

97 TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.

98 Euractiv. Greek MEP spyware scandal takes new turn.

COMP 47 (Paragraph 49 to Paragraph 49 a (new))

Covered: AM 430 (Rapporteur), AM 431 (Left)

Fall: AM 428 (ID), AM 429 (EPP)

49. Interestingly employees of Krikel have been spotted working at Ketyak, allegedly ‘pro bono’. Ketyak has ~~apparently~~ reportedly been granted €40 million from the EU’s Recovery and Resilience Facility ~~RRF~~, through a confidential tender procedure based on a secret decision of the Prime Minister^{1a}. ***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. (431).***

49 a (new). Reportedly, Krikel employees have also been visiting 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^{1b}. (430)

Footnotes:

1a. <https://www.flash.gr/politiki/1988373/predator-apokalypseis-gia-to-ketyak-tis-eyp-me-xrimatodotisi-kai-apo-to-tameio-anakampsis>

1b Inside Story. Greek State and spyware vendor Intellexa: they are acquainted after all.

COMP 48 (Paragraph 50 to Paragraph 50 a (new))

Involvement of Bitzios and Lavranos

Covered: AM 435 (Rapporteur), AM 436 (Left)

Fall: AM 432 (ECR), AM 433 (ECR), AM 434 (ID),

50. 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 administrator of Krikel in October 2017⁹⁹. Bitzios’ company Viniato Holdings Limited was subsequently hired as a consultant by Krikel between January and August 2018 for a fee of approximately 550 000 euros (although Krikel only had a turnover of 840 000 euro that year)¹⁰⁰.

Footnotes:

99 TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.
100 InsideStory. From Koukakis to Androulakis: A new twist in the Predator spyware case.

50 a (new). Bitzios and Pelczar have other mutual business connections as well. It emerges from the Paradise Papers that they share a company registered on Malta by the name of Baywest Business^{1a}. In addition, Tal Dilian, the founder of Intellexa holds a Maltese (golden) passport^{1b} and also has a letterbox company MNT Investments LTD in the island state^{1c}. (435, 436).

Footnotes:

1a International Consortium of Investigative Journalists. Offshore Leaks Database. Paradise Papers - Malta Corporate Registry

1b 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>

1c <https://mlt.databasesets.com/company-all/company/73006> <https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/>

COMP 49 (Paragraph 51 to Paragraph 52)

Covered: AM 437 (Left.), AM 438 (Greens.), AM 439 (Rapporteur)

Fall:

51. Bitzios and Lavranos are two key figures in the supply of communication and surveillance material to state bodies like police and EYP. Bitzios was pivotal in the company that sells Predator. They were close to Dimitriadis and they both benefited from lucrative government contracts. They benefitted 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 conflict 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.

51 a (new). 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 (438, 439) to summon these individuals for a hearing. (437).

Legal Framework

Paragraph 52

Covered:

Fall:

~~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.~~

COMP 50 (Paragraph 53 to Paragraph- 53 b (new))

Ex-ante scrutiny

Covered: AM 440 (S&D), AM 441 (Greens), AM 442 (Rapporteur), AM 443 (Greens), AM 444 (Rapporteur), AM 445 (Left),

Fall:

53. In Greece, infecting a device with spyware is a criminal offence as stipulated in several articles of the Greek Criminal Code, including art. 292 on Crimes against the security of telephone communications, art. 292B on hindering the operation of information systems as well as art. 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 art. 292C of the Greek Criminal Code¹⁰¹. ***This article was changed by the Greek government on 9 December 2022. (440).***

Footnote:

101 ICLG. *Cybersecurity Laws and Regulation Greece 2022*

53 a (new). The number of authorised wiretaps has increased substantially over the years. From 4871 in 2015, to 11,680 in 2019 to 15,475 in 2021^{1a}. Currently, some 60 requests have 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 nor the reason for the lifting of confidentiality. They are limited to the telephone number and the invocation of national security^{1b}. (441, 442, 445)

Footnotes:

1a Ekathimerini. *Wiretapping and 'national security'.*

1b Reporters United. *Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*

53 b (new). The judicial authorisation to monitor private communication 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^{1a}. Vlachou did not meet with the PEGA mission to Greece. (443, 444, 445).

Footnote:

1a Reporters United. *Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*

COMP 51 (Paragraph 54 to Paragraph 54 a (new))

Act of Legislative Content

Covered: AM 449 (Greens), AM 450 (Rapporteur)

Fall: AM 446 (ID), AM 447 (EPP), AM 448 (EPP)

54. 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 governor¹⁰². 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 Demiris as new EYP governor, whilst all other opposition parties were against¹⁰³. Incidentally, 2nd deputy commander of the EYP is Dionysis Melitsiotis¹⁰⁴, a former member of the private office of the Prime Minister, and another Deputy Director is Anastasios Mitsialis, a former Nea Demokratia official¹⁰⁵.

Footnotes:

102 Efsyn. What (does not) change with the Act of Legislative Content for EYP.

103 Kathemirini. Themistoklis Demiris: His appointment to the management of EYP was approved by a majority.

104 Ekathimerini. National security takes center stage.

105 Greek City Times. Greek PM appoints new security and intelligence chiefs.

54 a (new). In addition, the act reintroduced the two-prosecutor authorisation of monitoring requests^{1a}. 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 of by the Public Prosecutor of the Court of Appeals^{1b}. (449, 450).

Footnotes:

1a European Parliament. Greece's PredatorsGate: The latest chapter in Europe's spyware scandal?

1b Efsyn. What (does not) change with the Act of Legislative Content for EYP.

COMP 52 (Paragraph 55 to Paragraph 55 b (new))

Ex-post scrutiny

Covered: AM 451-A (Left), AM 454 (Greens), AM 455 (Rapporteur), AM 456 (Greens), AM 457 (Rapporteur)

Fall: AM 452 (ID), AM 453 (EPP)

55. Since 2019, the actions of the EYP have been under the direct control of Prime Minister Kyriakos **Mitsotakis (451)** after a change in the law following the victory of New Democracy in 2019¹⁰⁶.

Footnote:

106 Euractiv. Another Greek opposition lawmaker victim of Predator.

55 a (new). Parliamentary control is exercised by the Permanent Committee on Institution 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^{1a}. The

governing party has an absolute majority in the current committee composition (451, 454, 455).

Footnote:

1a Centre for European Constitutional Law. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies.

55 b (new). The Hellenic Authority for Communication Security and Privacy (ADAE) ensures the protection of confidentiality of mail and all other sorts of communications^{1a}. The statute of ADAE grants it administrative autonomy^{1b}. ADAE can carry out investigations at facilities, databases, archives, technical equipment and documents of the EYP^{1c}.(451, 456, 457)

Footnotes:

1a ADAE. Presentation

1b ADAE. Regulatory framework.

1c Centre for European Constitutional Law. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

COMP 53 (Paragraph 56 to Paragraph 56 c (new))

Covered: AM 458 (S&D.), AM 459 (Ernst, Kouloglou, et al.), AM 460 (Rapporteur), AM 461 (Left), AM 462 (Left), AM 468 (Greens)

Fall: AM 463 (Left)

56. 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 the inquiry of 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 compromised¹⁰⁷. 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 2472/1997¹⁰⁸. However, when in March 2021 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 communications¹⁰⁹. This de facto strips the individual of its right to information. The amendment was introduced in a highly irregular manner. It was added to ~~an totally~~ unrelated law (a bill to do with covid measures) and the deadlines required by the Constitution were not respected^{110 111 112}. There was therefore no proper consultation process.

Footnotes:

107 Constitutionalism. Contradiction of article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications.

108 Dpa. Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data.

109 <https://www.reportersunited.gr/8646/eyp-koukakis/>

110 Hellenic Parliament. Constitution.

111 Hellenic Parliament. Rules of Procedure of the House.

112 Govwatch. Violation of the legislative process for amendments in law 4790/2021.

56 a (new). With the Act of Legislative Content, Mitsotakis aimed to strengthen transparency and accountability. Yet, the act does not revoke Amendment 826/145 (460, 468).

56 b (new). On 9 December 2022, the Greek government adopted law 5002/2022 with the aim to update and create 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 stipulated in Article 4 Paragraph 7^{1a}, 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 (458). Additionally, it makes it practically impossible for individuals that are under surveillance on national security grounds to be appropriately informed *ex post*, as this 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^{1b} (459) 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^{1d}. 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, nor for subcontracting wiretapping to private entities (461).

Footnote:

1a. <https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022>

1b. <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>

1c. <https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022>

1d. PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.

56 c (new). 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 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 an 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 par. 1 of the Constitution, which calls for a narrow interpretation. 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 (462).

COMP 54 (Paragraph 57)

Covered: AM 464 (Greens), AM 465 (Rapporteur)

Fall: AM 466 (ID), AM 467 (Left),

57. The possibilities for ex-post scrutiny ~~are further~~ were weakened by the fact that Greece ~~has still not~~ **took a long time to** fully implemented the EU Whistleblowers Directive¹¹³. **On 27 January 2022, the Commission launched an infringement procedure by sending a formal notice to Greece. On 15 July 2022, the Commission sent a reasoned opinion with a deadline of two months to reply. (464, 465). The Greek Parliament eventually voted law 4990/2022 on 11 November 2022, transposing the EU Whistleblowers Directive into the Greek legislation.**

Footnotes:

113 https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768

113a https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768

COMP 55 (Paragraph 58)

Public scrutiny

Covered: AM 362 (Left), AM 469 (Rapporteur), AM 470 (Greens)

Fall:

58. Greece ranks lowest of all EU countries in the World Press Freedom Index 2022: 108 out of 180¹¹⁴. In 2021, journalist Giorgos Karaivaz was murdered. The murder has still not been resolved. Journalists face intimidation and SLAPPs. Grigoris Dimitriadis¹¹⁵ launched Strategic Lawsuits against Public Participation (SLAPPS) against news outlets Reporters United and Efimerida ton Syntakton (EfSyn)¹¹⁶ 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 motivated¹¹⁷. Indeed two of the **targets of surveillance (470)**, 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 surveillance¹¹⁸. **In addition, Greece's Supreme Court Prosecutor Isidoros Dogiakos discredited media outlets that criticized the Greek judicial authorities for not handling the Greek wiretapping scandal adequately (AM 469). He even attempted to intimidate the media investigating the scandal by requesting selective tax audits for their owners^{118a} (362).**

Footnotes:

114 <https://rsf.org/en/index>

115 Tagesspiegel.

116 EUobserver. Greece accused of undermining rule of law in wiretap scandal.

117 <https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/>

118 Heinrich-Böll-Stiftung. *In conditions of absolute loneliness.*

118a ESIEA Journalists Unions condemn threats from Supreme Court Prosecutor <https://www.esiea.gr/oι-dimosiografikes-enoseis-gia-tis-di/>

COMP 56 (Paragraph -59 a (new) to Paragraph 59)

Redress

The National Transparency Authority

Covered: 471 (Greens), AM 472 (Rapporteur), AM 473 (Left)

Fall:

-59 a (new). *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 National Transparency Authority 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^{1a}. (471, 472, 473). Whilst the ADAE's independence is stipulated in the constitution, the EAD is not an independent authority.*

Footnote:

1a <https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019>

59. On 22 July 2022, the National Transparency Authority (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. 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 cloak of personal data protection, several names of 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 involved¹¹⁹.

Footnote:

119 InsideStory. *From Koukakis to Androulakis: A new twist in the Predator Spyware case.*

COMP 57 (Paragraph 60)

Covered: AM 474 (Rapporteur)

Fall:

60. ***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 spyware¹²⁰. However, the EAD did not investigate the bank accounts of Intellexa and Krikel, nor the affiliated offshore companies. In addition, the ***EAD*** only visited the offices of Intellexa and Krikel after 2 months ***since the first publication about the use of Predator in Greece***, at which point employees were working home due to COVID. The EAD furthermore did not meet with legal representatives of the companies in question.¹²¹ (474)

Footnote:

120 InsideStory. From Koukakis to Androulakis: A new twist in the Predator Spyware case.

121 InsideStory. From Koukakis to Androulakis: A new twist in the Predator Spyware case.

COMP 58 (Paragraph 61)

Covered:

Fall: AM 475 (EPP)

61. There are question marks over the independence of the EAD leadership. ~~Recently EAD made headlines with suggestions of pro-government bias in drawing up a report on migrant pushbacks¹²².~~ The ***current*** Director of EAD, 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 on spyware in Greece.***

Footnote:

122 ~~<https://www.politico.eu/article/greek-transparency-agency-report-data-breach-migration-european-commission>~~

COMP 59 (Paragraph 62 to Paragraph 62 f (new))

The Hellenic Authority for Communication Security and Privacy (ADAE)

Covered: AM 364 (Left), AM 367 (Left), AM 476 (S&D), AM 477 (Left.), AM 478 (Greens), AM 479 (Rapporteur), 482 (Greens), AM 483 (Rapporteur), AM 484 (S&D), AM 485 (Rapporteur), AM 486 (Rapporteur), AM 487 (Rapporteur)

Fall:

62. 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 the 21st of September 2021. Following Androulakis' complaint the ADAE launched an inquiry in August 2022, starting with obtaining information from Androulakis' telecom operator.

62 a (new). *Predator spyware leaves few traces of infection at the telecommunications providers. (479) However, the ADAE found that the mobile phone of Androulakis was monitored by the EYP^{1a}, 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 (477, 478, 479).*

Footnote:

1a [https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA\(2022\)733637_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf)

62 b (new). *Following the findings of the ADAE inquiry Grigoris Dimitriadis and Panagiotis Kontoleon, resigned from their government positions^{1a}. Kontoleon stated that the monitoring of Androulakis was set off at the request of foreign authorities - more specifically the Intelligence agencies of Armenia and Ukraine - in light of Androulakis' partaking in the European Parliament committee on trade relations between the European Union and China^{1b}. Both Ukraine and Armenia have repudiated these claims^{1c} (477, 482, 483).*

Footnotes:

1a POLITICO. PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal

1b <https://www.kathimerini.gr/politics/561988786/ypothesi-parakoloythiseon-ta-dedomena-poy-pyrodotisan-tis-exelixeis/>

1c European Parliament. Greece's PredatorsGate: The latest chapter in Europe's spyware scandal?

62 c (new). *On 15 December 2022, the authority followed up on requests from journalists Tasos Telloglou and MEP Giorgos Kyrtos on whether they were targeted by the EYP. An audit by the ADAE into the telecommunication's company Cosmote found that both Telloglou and Kyrtos were indeed under surveillance^{1a}. Cosmote informed the Supreme Court and questioned the legality of the ADAE's investigation^{1b}. ADAE set up a special team to scrutinize the telecommunication providers, specifically looking for further requests made by the EYP for the lifting of confidentiality^{1c}. (485)*

Footnotes:

1a Euractiv. Exclusive: Another MEP and journalist the latest victims of 'Greek Watergate'

1b International Press Institute. Greece: MFRR alarmed by latest revelations of spying on journalists.

1c Euractiv. Privacy watchdog to scrutinize telecoms companies over 'Greek Watergate'

62 d (new). *The government has attempted to replace the members of the ADAE's Board of Directors (476). 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 telecommunication providers to look into the lifting of the confidentiality of communications. According to this Opinion, criminal sanctions could apply once the ADAE starts such audits^{1a}. This opinion, which contradicts previous opinions of the Attorney General, clearly violates the independence of the ADAE^{1b} and tries to prevent it from conducting investigations (476, 486). During a PEGA Committee meeting on 28 February 2023, Rammos stated that the Opinion of Dogiakos is not binding and the tasks of the ADAE can carry on as usual^{1c}.*

Footnotes:

1a Euractiv. Chief prosecutor puts Greece's rule of law to the test

1b <http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bdilosi-toy-proedroy-tis-adae-christoy-rammoy-gia-tin-g/>

62 e (new). *The ADAE has confirmed that the EYP has also spied upon the head of the Greek armed forces Konstantinos Floros, a serving minister, several officers that deal with arm cases and a former national security advisor. Due to the current inability of the ADAE to inform the victims, the ADAE intended to present the findings to the parliament's transparency committee and the parliament's institutions^{1a}. Christos Rammos sent a letter to the Parliament 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 (364). Eventually the ND majority within the Committee on Institutions and Transparency denied his request (487). On 24 January 2023, the Spokesperson of the Government attacked the ADAE and its president for its investigations^{1a} (484), arguing that Rammos was performing "activism" and "overstepping" his mandate (367) 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 Parliament, confirming that The Head of the Armed Forces, 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 (367). Given the seriousness of the findings, the refusal to allow ADAE to report to Parliament and the discrediting of the authority amount to the obstruction of accountability and transparency^{1b}. (487, 484)*

Footnotes:

1a <https://www.protothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosisuni-o-prothupourgios-den-gnorize-to-paramikro/AMP/>, <http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/>;

1b Newsbomb. SYRIZA: Maximos "circles" through ADAE - What he sees behind the "blockade" of ND in Rammos.

62 f (new). *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 its operational framework for complaints and investigations. Rammos mentioned that the ADAE receives approximately 10 complaints per day.^{1a}*

Footnote:

1a. PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.

COMP 60 (Paragraph 63 to Paragraph 65)

The Committee on Institutions and Transparency

Covered: AM 488 (Greens), AM 489 (Rapporteur), AM 490 (Greens), AM 491 (Rapporteur), AM 492 (Left)

Fall:

63. In July 2022, the Committee on Institutions and Transparency ~~had~~ 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 upon 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 spyware¹²³.

Footnote:

123 Reuters. Greek intelligence service admits spying on journalist - sources.

63 a (new). Although the meetings are in camera^{1a} reportedly neither Kontoleon nor Dimitriadis were willing to provide substantial evidence, invoking national secrecy reasons^{1b}. The new head of EYP Demiris denied the committee access to a report containing information on the alleged destruction of surveillance data^{1c}. This effectively means that the EYP refuses accountability and the Parliament cannot carry out its mandate of parliamentary oversight (488, 489, 492).

Footnotes:

1a Ekathimerini. Transparency committee to hold closed-door meeting on phone hacking allegation.

1b Tovima. In combat positions for eavesdropping.

1c Tovima. In combat positions for eavesdropping.

63 b (new). On 30 August, the committee summoned nine people for a closed-door hearing, including public prosecutor Vasiliki Vlachou, former Secretary General Grigoris Dimitriadis and former head of EYP Kontoleon. All of them invoked confidentiality and avoided answering questions during this committee hearing^{1a}. (490, 491 492).

Footnote:

1a 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-syngkalypsi>

The Parliamentary Committee of Inquiry

Paragraph 64

Covered:

Fall:

64. A proposal by the PASOK-KINAL party to set up a committee of inquiry into the alleged use of spyware¹²⁴ was endorsed by 142 MPs of the opposition, while the 157 Nea Demokratia MPs abstained¹²⁵. However, ND had an absolute majority in the inquiry committee. 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.

Footnote:

124 Tovina. Interceptions: Committee of Inquiry to monitor Androulakis - Pasok's proposal in detail.

125 Tovina. Parliament: The examination for the attendances from 2016 was passed - With 142 'yes'.

Paragraph 65

Covered:

Fall:

65. The government majority in the committee refused to invite Bitzios and Lavranos, but it did invite Stamatis Tribalís - current manager of Krikel - and Sara Hamou. On 22 September, Tribalís testified in front of this parliamentary committee. Tribalís presented blatantly false information about the involvement of Bitzios and Lavranos in Krikel, claiming i.a. that he himself was the owner of Krikel¹²⁶.

Footnote:

126 TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.

COMP 61 (Paragraph 66 to Paragraph 66 e (new))

Covered: AM 451-B (Left), AM 480 (S&D), AM 493 (Left), AM 495 (Greens), AM 496 (Rapporteur), AM 497 (Rapporteur), AM 498 (Rapporteur), AM 499 (Rapporteur),

Fall: AM 481 (Left), AM 494 (EPP), AM 500 (Rapporteur)

66. 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. ~~As~~ Common conclusions could not be reached ***due to severe polarisation of the political landscape, each party published its own report. A government-led majority decided to classify*** some 5 500 pages of documents, including the minutes and the deposition of Hamou ~~have been classified, and the main findings of the parties,~~ although it is entirely within the powers of Parliament to declassify them ***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. Quite paradoxically, the inquiry committee thus serves to shield information, instead of providing access to it.***

66 a (new). The opposition proposed some other witnesses, such as Koukakis, Mitsotakis, Dimitriadis, Vlachou, Lavranos, and Bitzios but the committee eventually denied to invite them. On 10 October 2022, the committee finished its investigations and the different political parties all submitted their final reports^{1a}. (496, 495, 493).

Footnote:

1a Ieídiseis. SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.

The Hellenic Data Protection Authority (497)

66 b (new). The Hellenic Data Protection Authority (APDPX) is an independent authority and has the role to supervise the application of the GDPR, other regulations and national laws concerning data protection of the individual in Greece^{1a} (451, 498). The 4624/2019 law excluded national security from the remit of the APDX, while it had been included since the law of 1997.^{1b} Following the complaint by Nikos Androulakis in July 2022 (480), 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. (480, 498). 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 with much delay, thus obstructing the audit of the authority^{1c} (498).

Footnotes:

1a Hellenic Data Protection Authority. https://www.dpa.gr/en/enimerwtiko/legal_framework/personal_data

1b. Government Gazette of the Hellenic Republic. https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDP.A.PDF

1c Hellenic Data Protection Authority. Imposition of a fine on Intellexa S.A. for non-cooperation with the Authority.

66 c (new). On 16 January 2023, the authority fined Intellexa S.A. for this obstruction and their unwillingness to cooperate during the audit for 50.000 euros^{1a}(499) on the basis of Article 31 of the GDPR.

66 d (new). Following the action undertaken by the APDPX, Intellexa has handed over documents but the authority is still looking into them. According to President of the APDPX Menoudakos, the authority did discover domain names that possibly belong to companies cooperating with Intellexa within and outside the EU. The investigation of the authority is still ongoing^{1b}.

Footnote:

1a Hellenic Data Protection Authority. Imposition of a fine on Intellexa S.A. for non-cooperation with the Authority

1b . PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.

66 e (new). During a PEGA Committee meeting on 28 February 2023, the president of the authority mentioned that a APDPX inquiry looked into internet applications for sending text messages. According to Menoudakos, companies have made use of these internet applications to deliver text messages related to the Predator spyware. The authority is currently trying to identify the targets but has so far confirmed that 300 text messages have been sent to approximately 100 receivers by means of this method. The APDPX has instructed the companies for the non-destruction of this data and underlined that if these companies have no legal representative in the EU, they are violating the GDPR^{1a}.

Footnote:

1a. PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.

COMP 62 (Paragraph 67)

The Targets

Covered:

Fall: AM 501 (EPP), AM 502 (ECR)

~~67. At the time of writing, a list of 33 names of targets had been published. It is not possible to make the detailed analysis and no formal investigations have been launched yet. However, the analysis of the handful of cases known so far does provide a fairly clear image of the issues at hand~~

COMP 63 (Paragraph 68 to Paragraph 68 h (new))

Thanasis Koukakis

Covered: AM 503 (Left), AM 505 (Left), AM 506 (Greens), AM 507 (Rapporteur), AM 508 (Left), AM 509 (Greens), AM 510 (Rapporteur), AM 511 (Left) AM 512 (Greens), AM 513 (Rapporteur), AM 514 (Left) AM 515 (Greens), AM 516 (Rapporteur), AM 517 (Greens), AM 518 (Rapporteur), AM 519 (Greens), AM 520 (Rapporteur), AM 521 (Greens), AM 522 (Rapporteur), AM 523 (Greens), AM 524 (Rapporteur).

Fall: AM 504 (ECR)

68. 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 businessmen Yiannis Lavranos, and on controversial banking laws introduced by the Mitsotakis Greek government impeding the prosecution of money laundering and other financial wrongdoing (indeed the retroactive effect led to twelve pending cases being dropped)¹²⁷. Koukakis was also investigating the procurement for new ID cards, where Lavranos and Bitzios had a business interest. Around the time of Koukakis first appearance before PEGA, the tender was suddenly withdrawn and the responsible General Secretary resigned.

Footnote:

127 Inside Story. Who was tracking the mobile phone of journalist Thanasis Koukakis.

68 a (new). On 29 July 2022 EYP chief, Panagiotis Kontoleon declared that the EYP had monitored Koukakis' phone in light of 'national security reasons'. (506, 507, 503)

68 b (new). On 1 June 2020, the EYP submitted a first request to lift the confidentiality of the telephone number of Koukakis for two months, until 1 August 2020. EYP submitted a request for an extension by an additional two months^{1a}, i.e. until 1 October 2020. The Prosecutor of the Court of Appeals - Vasiliki Vlachou - has approved all these provisions under the invocation of national security^{1b}. (510, 509, 505)

Footnotes:

1a Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis.

1b Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis; Inside Story. Who was watching journalist Thanasis Koukakis' cell phone?

68 c (new). However, twelve days later, on August 12, 2020, the EYP suddenly requested the termination of the lifting of the confidentiality of Koukakis' telephone number, i.e. a month and a half earlier than foreseen in the original request. That happened on the same day when Koukakis approached ADAE with the request to be informed about the possible monitoring of his two mobile phones and a landline. (505, 513, 512).

68 d (new). 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^{1a}. The president of ADAE Christos Rammos and two other members of the ADAE have argued against this amendment, pointing out in an OpEd that the amendment violates the right to respect for private and family life of the European Convention on Human Rights

(ECHR) and the protection of confidentiality of communications as guaranteed in the Constitution^{1b}. (508, 515, 516)

Footnotes:

1a 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. *Who was watching journalist Thanasis Koukakis' cell phone?* <https://insidestory.gr/article/poios-parakoloythoyse-kinito-toy-dimosiografoy-thanasi-koykaki>

1b 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/tag/%25CE%25B1%25CF%2581%25CF%2587%25CE%25AE-%25CE%25B4%25CE%25B9%25CE%25B1%25CF%2583%25CF%2586%25CE%25AC%25CE%25BB%25CE%25B9%25CF%2583%25CE%25B7%25CF%2582-%25CF%2584%25CE%25BF%25CF%2585-%25CE%25B1%25CF%2580%25CE%25BF%25CF%2581%25CF%2581%25CE%25AE%25CF%2584%25CE%25BF%25CF%2585-%25CF%2584%25CF%2589%25CE%25BD-%25CE%25B5%25CF%2580/>

68 e (new). Between 12 July 2021 and 14 September 2021 the telephone of Koukakis was infected with Predator spyware^{1a}. According to Koukakis, he received a text message with a link to a financial news webpage^{1b}. On 28 March 2022, Citizen Lab officially revealed the infection^{1c}. (517, 518, 511).

Footnotes:

1a Inside Story. *Who was watching journalist Thanasis Koukakis' cell phone?*

1b European Parliament. *Hearing September 8, 2022.*

1c Inside Story. *Who was watching journalist Thanasis Koukakis' cell phone?*

68 f (new). Koukakis made several attempts to find redress for the surveillance attempts. He filed two complaints with the ADAE. The first one on 6 April 2022 where he requested a thorough inquiry into the Predator contamination of his mobile phone. The second one on 13 May 2022 in light of the new revelations as published by InsideStory and Reporters United. In addition, Koukakis filed a complaint with the EAD on 4 May 2022, where he requested an investigation into the background of the interceptions by the EYP and the Predator attack^{1a}. (519, 520, 511).

Footnote:

1a Avgi. *Thanasis Koukakis / Filed a lawsuit for the Predator – Who and why was watching him*

68 g (new). 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^{1a}. The Cyprus and Ireland subsidiaries of Intellexa were not investigated at all^{1b}. The investigations did not include information on the bank accounts of Intellexa and subsidiaries^{1c}. Koukakis appealed to the European Court of Human Rights on 27 July 2022^{1d}. (521, 522, 514).

Footnotes:

1a InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*

1b InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*

1c InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*

1d BBC. *Greece wiretap and spyware claims circle around PM Mitsotakis*

68 h (new). *On 5 October 2022, Koukakis filed a complaint with prosecutors in Athens against Intellexa Alliance, and particularly Tal Dilian and Sara Hamou^{1a}, for violating the confidentiality of his communications^{1b}. (523, 524, 514)*

Footnotes:

1a News 24 7. Wiretapping scandal: Lawsuit against Intellexa by Thanasis Koukakis.

1b Heinrich Boll Stiftung. In conditions of absolute loneliness.

COMP 64 (Paragraph 69 to paragraph 69 h (new))

Nikos Androulakis

Covered: AM 525 (Left), AM 526 (Left), AM 527 (Greens), AM 528 (Rapporteur), AM 529 (Left), AM 530 (Rapporteur), AM 531 (Greens), AM 532 (Rapporteur), AM 533 (Greens), AM 534 (Rapporteur), AM 535 (Greens), AM 536 (Rapporteur), AM 537 (Greens), AM 538 (Rapporteur), AM 539 (Greens), AM 540 (Greens), AM 541 (Rapporteur), AM 542 (Rapporteur).

Fall:

69. On September 21, 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 telephone¹²⁸. 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 Koukakis, Androulakis did not click on the link that was sent to him¹²⁹. ***During a PEGA Committee meeting on 28 February 2023, Androulakis stated that the APDPX identified the credit card account that paid for the text messages sent to him. This information was shared with the relevant prosecutor^{1a}.***

Footnotes:

128 InsideStory. From Koukakis to Androulakis: A new twist in the Predator spyware case.

129 Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.

1a. PEGA Committee Exchange of Views with Konstantinos Menoudakos and Christos Rammos. 28.02.2023.

69 a (new). *In July 2021, Androulakis’ announced his candidacy in the race for party leadership^{1a}. According to the ADAE inquiry, the mobile phone of Androulakis was at that time monitored by the EYP through the telecommunications providers^{1b}. EYP Prosecutor Vasiliki Vlachou approved the lifting of secrecy of Androulakis’ phone on “national security” grounds. The approval coincided with both the Predator targeting and Androulakis’ candidacy. (525, 527, 528).*

Footnotes:

1a Tovima. Androulakis lashes out at PM, ND spokesman says Pasok leader should say why his phone was tapped

1b Kathimerini. Surveillance hypothesis: the data that triggered the developments.

69 b (new). *When Androulakis was elected party leader in December 2021, the “official” EYP monitoring was terminated abruptly^{1a}, despite the fact that the two-month re-authorisation for his surveillance had not yet expired. (525, 530, 531)*

69 c (new). *On 28 June 2022, DG ITEC of the European Parliament checked Androulakis’ phone and found the evidence of the attempted Predator hack of September 2021, and*

informed Androulakis accordingly^{1a}. Androulakis filed a criminal report to the prosecutor's office of the Supreme Court on 26 July 2022^{1b}. (532, 533, 526).

Footnotes:

1a Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.

1b News 247. Nikos Androulakis: Near-Victim of Predator Software - Filed a Lawsuit.

69 d (new). A few days later, on 29 July, Androulakis presented the information about the Predator attack to the ADAE. At 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^{1a}. (534, 535, 526).

Footnote

1a Avgi. Predator scandal / EYP dragged to Parliament over surveillance

69 e (new). On 8 September 2022, Androulakis asked the ADAE to hand over his wiretapping files^{1a}. However, on this same day, Ta Nea reported on an official briefing from the ADAE mentioning ~~it becomes clear~~ that the files of both Androulakis and Koukakis were destroyed by the EYP^{1b}. 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^{1c}. 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 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^{1d}. (536, 537, 529). During a PEGA Committee hearing, President of the ADAE Rammos did not confirm nor deny the destruction of records^{1e}.

Footnotes:

1a Ekathimerini. Androulakis asks ADAE for his wiretapping file.

1b TaNea. The archive of the surveillance of Nikos Androulakis destroyed.

1c TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.

1d Ieidiseis. SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.

1e. European Parliament. Hearing September 8, 2022.

69 f (new). On the 5th of August, Kontoleon and Dimitriadis resigned from their positions. On the 8th of August Mitsotakis made a television statement, acknowledging the wiretapping of Androulakis, but reiterating the fact that he was unaware of the surveillance^{1a}. (538, 539, 529)

Footnote:

1a Reuters. Greek PM says he was unaware of phone tapping of opposition party leader

69 g (new). EYP has so far declined to disclose the reasons for the surveillance. It has offered to inform Androulakis privately of the reasons. This would be unlawful. Androulakis requested for his surveillance file to be submitted to the Committee on Institutions and Transparency, but that was rejected. (540, 541, 529).

69 h (new). On 7 December 2022, 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^{1a}. (542)

Footnote:

1a Ekathimerini. Socialist leader appeals to European Court over tapping

COMP 65 (Paragraph 70)

Covered:

Fall: AM 543 (S&D), AM 544 (EPP),

70. Surveillance of a politician is highly unusual, and the Greek Constitution foresees 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 Androulakis, or they suggested that his 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. ~~Polls predicted that Néa Demokratía would lose its absolute majority.~~ PASOK would be the preferred coalition partner. In autumn 2021, there were four candidates in the PASOK leadership contest, each with different views on such a coalition. Androulakis was said to be open to the idea, but not under the Premiership of 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 to Dimitriadis. ~~Manolis Othonas, the right hand of another candidate, was also said to be among those who had closer relations with Néa Demokratía and 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.

COMP 66 (Paragraph -71 a (new) to Paragraph -71 b (new))

Giorgos Kyrtzos

Covered: AM 545 (Rapporteur), AM 546 (Rapporteur), AM 547 (Rapporteur),

Fall:

-71 a (new). On 15 December 2022, an ADAE audit into Cosmote telecommunications company confirmed that Member of European Parliament Giorgos Kyrtzos was under surveillance by the EYP^{1a}. Both his mobile phones and his landline were wiretapped. The surveillance was reportedly prolonged nine times^{1b} for a period of 18 months (546).

Foonotes:

1a Euractiv. EXCLUSIVE: Another MEP and journalist the latest victims of ‘Greek Watergate’.

1b Politico. Greek prosecutor slams unflattering comparisons to Belgium’s Qatargate probe.

-71 b (new). Giorgios Kyrtzos ~~was~~ is a former member of Nea Demokratia and the European People’s Party. In February 2022, ND expelled Kyrtzos from the Greek ruling party due to his disapproval of the government’s action surrounding the Covid-19 pandemic, media freedom restraints and the approach to the Novartis scandal^{1a}. After his expulsion, Kyrtzos joined Renew Europe. (547).

Footnote:

1a Euractiv. *Renew Europe welcomes first Greek MEP who left EPP.*

COMP 67 (Paragraph 71 - 71 b (new))

Stavros Malichoudis

Covered: AM 548 (Left), AM 549 (Rapporteur), AM 550 (Greens), AM 551 (Rapporteur), AM 552 (Greens),

Fall:

71. 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^{130 131}. Malichoudis was writing about a 12-year-old Syrian child that was coerced to live for several months in a detention camp on the Greek island Kos¹³².

Footnotes:

130 Efsyn. *Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ*

131 Solomon. *Solomon's reporter Stavros Malichoudis under surveillance for 'national security reasons'.*

132 BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*

71 a (new). *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"^{1a}. However, on 24 November and 17 December 2021, Minister of State George Gerapetritis denied any surveillance of journalists in Greece, including of Malouchidis, but according to media outlet Solomon he neither confirmed nor denied ~~did not deny~~ the authenticity of the EYP internal documents^{1b}. (549 548, 550)*

Footnotes:

1a BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*

1b <https://wearesolomon.com/mag/accountability/solomons-reporter-stavros-malichoudis-under-surveillance-for-national-security-reasons/>

71 b (new). *During the PEGA hearing on Greece on 8 September 2022, 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^{1a}. The EYP could have allegedly listened in on conversations Malichoudis had with the International Organisation for Migration (IOM)^{1b}, pointing out the dangers for others, the so-called 'by-catch', of wiretapping an individual. In addition, during the hearing 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"^{1c}. (551, 552, 548).*

Footnotes:

1a European Parliament. *Hearing September 8, 2022*

1b BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*

1c European Parliament. *Hearing September 8, 2022*

COMP 68 (Paragraph 72)

Christos Spirtzis

Covered: AM 553 (Left), AM 554 (Rapporteur), AM 555 (Greens),

Fall: AM 556 (ECR),

72. On ~~15 November 2021~~ **9 September 2022** former Minister of Infrastructure and lawmaker for the Syriza party Christos Spirtzis *claimed to have been* ~~was~~ targeted with the Predator spyware on his mobile phone¹³³. *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^{133a} 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^{133b}. Whilst CitizenLab did not check these messages, Spirtzis did share the links he received with two technicians who verbally confirmed that he had been targeted^{133c}. On 9 September 2022, Spirtzis lodged a complaint to the prosecutor of the Supreme Court^{133d}. Spirtzis is a confidante of party leader Tsipras, and present during high-level meetings of the party leadership. (553, 554, 555).*

Footnotes:

133 Ekathimerini. Former SYRIZA minister says he was targeted by Predator.

133a. <https://govwatch.gr/en/finds/apopeira-parakolythisis-toy-christoy-spirtzi-me-to-paranomo-logismiko-ypoklopon-predator/>

133b Ekathimerini. Former SYRIZA minister says he was targeted by Predator

133c. <https://insidestory.gr/article/predator-perissoteroi-apo-20-oi-stohoi-toy-stin-ellada-symfona-me-tin-arhi-prostasias>

133d Reuters. One more Greek lawmaker files complaint over attempted phone hacking; Euractiv. Another Greek opposition lawmaker victim of Predator.

COMP 69 (Paragraph 73 - 73 b (new))

Tasos Telloglou, Eliza Triantafyllou and Thodoris Chondrogiannos

Covered: AM 557 (Left), AM 558 (Greens), AM 559 (Rapporteur), AM 560 (Rapporteur), AM 561 (Greens), AM 562 (Rapporteur)

Fall:

73. **Journalists** Tasos Telloglou and Eliza Triantafyllou have allegedly been spied upon during their investigative work for the **news outlet** Inside Story. *In an article for the Heinrich-Böll-Stiftung on 24 October 2022, Telloglou shared his surveillance and intimidation experiences whilst investigating the surveillance scandals in Greece. According to these experiences, he believes to have been monitored between May and August 2022^{1a}. (557, 558, 559)*

Footnote:

1a Heinrich-Böll-Stiftung. In conditions of absolute loneliness

73 a (new). *In addition, a source from the security services had told Telloglou in June 2022 that the locations of him and his colleagues Eliza Triantafyllou (InsideStory) and Thodoris*

Chondrogiannos (Reporters United) were monitored by the authorities, to assess which sources they were meeting^{1a}. At time of writing, the Greek government has not yet responded to the allegations. (560, 561).

Footnote:

1a MapMF. Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations.

73 b (new). On 15 December 2022, an ADAE audit into Cosmote telecommunications company confirmed that Telloglou was under surveillance by the EYP. Due to ‘national security’, the reasons for the surveillance were not revealed^{1a}. (562)

Footnote:

1a Euractiv. EXCLUSIVE: Another MEP and journalist the latest victims of ‘Greek Watergate’.

COMP 70 (Paragraph 74 to Paragraph 75 f (new))

Covered: AM 360 (Left), AM 563 (Left), AM 565 (S&D), AM 566 (Rapporteur)

Fall: AM 564 (EPP)

Other targets

Covered:

Fall:

74. 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 Nέα Demokratía reportedly received a link for the instalment of Predator.¹ Oikonomou - government spokesperson - has stated that the article lacks concrete evidence.²

75. On 5 and 6 November 2022 Documento reported on a list containing 33 names of persons allegedly targeted with Predator spyware¹³⁶. Among them are 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 Kyrtos^{136a}, Chief of Joint Staffs General Konstantinos Floros^{136b}, Chief of the Hellenic Army Haralambos Lalousis^{136c}, Minister of Labour and Social Affairs Kostis Hatzidakis^{136d}, former General Directors of Defence Equipment and Investments Theodoros***

¹ Ta Nea. [Four illegal manipulations by suspicious center.](#)

² Politico. [Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.](#)

Lagios and Aristides Alexopoulos^{136e}, former security advisor Alexandros Diakopoulos^{136f} and Greek investigative journalist Tasos Telloglou^{136g} (AM 360, AM 565, AM 566).

Footnotes:

136 Documento, edition 6 November 2022; <https://www.politico.eu/article/greece-spyware-scandal-cybersecurity/>; <https://www.dw.com/en/wiretapping-scandal-in-greece/a-64128644>

136a. <https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watertgate/>

136b. https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyptoy-mitsotaki

136c. https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyptoy-mitsotaki

136d. <https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/>

136e. <https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/>

136f. <https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/>

136g. <https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watertgate/>

75 a (new). In addition, Meta's former Cybersecurity 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 her device was renewed 6 times, all of which in principle require approval from the EYP's in-house prosecutor 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 3 months after the conventional wiretapping started. Seaford stated that information on her Covid-19 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 official government system for vaccinations.

75 b (new). 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 during Seaford's role at Meta, a company that has published a threat-report on the surveillance-for-hire industry and banned multiple spyware companies from their platform, including Cytrox. 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 2022, much later than the timing of the targeting of Seaford's device, and none of the other people involved in writing the report were targeted themselves. In addition, Seaford stated^{1a} that she was only partly involved in these activities and that Meta is very discrete in communicating names of their employees.

Footnote:

1a. PEGA Committee Meeting, 20 April 2023.

75 c (new). *In March 2021, magazine Marie-Claire published an article including an interview with Seaford. The interview mentions Seaford's experiences with everyday sexism and harassment in Greece and it particularly describes a case of sexual harassment by "a politician"^{1a)}. 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. In this particular case the number of suspects can be narrowed down further, as clearly the perpetrator also had accomplices inside the government vaccination system.*

Footnotes:

1a. <https://www.marieclaire.gr/art-lifestyle/artemis-seaford-i-chiroteri-morfi-katapiesis-ine-afti-pou-den-katalavenis-oti-ifistase/>

75 d (new). *It is of importance that these possibilities are further investigated, in particular the question who requested the surveillance by the EYP. Seaford has filed a request with the ADAE and has lodged a complaint with the court in Greece. However the investigation is still in process. She is the first known American citizen to be targeted in the EU^{1a}.*

Footnote:

1a. <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.;PEGA Committee Meeting, 20 April 2023>

75 e (new). *Other names on the list that were not officially confirmed are Former Minister for Education and Religious Affairs Andreas Loverdos, former Prime Minister Antonis Samaras, Minister of State George Gerapetritis, Former Commission 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 Karamalakos, 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 (AM 360, AM 563). The revelations of the list are highly disturbing not just because of the high profile names on it but also because it suggests that the abuse of spyware is systematic, and large-scale. and part of a political strategy.*

75 f (new). *In 2023 ADAE reported that the EYP has also wiretapped a serving minister, several officers that dealt with arm cases and a former national security advisor^{1a}. (565, 566).*

Footnote:

1a. Politico. Brussels Playbook: Globalization's sanatorium - Vestager rings alarm - S(uspended & D(umped)

COMP 71 (Paragraph 75 g (new) to Paragraph 75 h (new))

Concluding remarks

Covered: AM 365 (Rapporteur), AM 373 (Left)

Fall: AM 368 (EPP), AM 369 (ECR), AM 370 (Rapporteur), AM 371 (Left), AM 372 (ID)

75 g (new). *There are patterns suggesting that the Greek government enables the use of spyware against journalists, politicians and businesspersons, the export of spyware to countries with poor human rights records, and provides a training centre for third country agents that want to familiarize themselves with spyware. Despite the fact that the use of spyware is illegal in Greece, a search for the origins of the spyware attacks only gained momentum in Summer 2022 (365). A political majority is reportedly being used for the advancement of particular interests rather than the general interest, notably by the appointment of associates and loyalists in key positions such as the EYP, EAD (National Transparency Authority) and Krikel (Company specialised in electronic security systems)(371). Whereas spyware, which in some cases happened in parallel or subsequently to legal interception, is used as a tool for political power and control in the hands of the highest political leadership of the country. 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 with respect to surveillance is inadequate, for the protection of citizens against abuse by both 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 (373).*

Covered:

Fall: AM 374 (ID), AM 375 (EPP), AM 376 (ECR), AM 378 (Rapporteur), AM 379 (Left), AM 380 (Greens)

75 h (new). *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 integral authoritarian strategy, but rather a tool used on an ad hoc basis for political and financial gains. However, it equally erodes democracy and the rule of law, and gives ample room to corruption, whereas these turbulent times call for reliable and responsible leadership.*

Compromises on Cyprus

COMP 72 (Paragraph -76 a (new) to Paragraph 77)

Covered: AM 568 (ID), AM 577 (Rapporteur), AM 578 (Greens), AM 579 (Greens), AM 580 (Rapporteur), AM 581 (Rapporteur)

Fall: AM 582 (ID)

-76 a (new). The Committee visited Cyprus in November 2022 as part of a joint mission Greece/Cyprus. Members met with 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 have presented the Committee with documentation as regards to surveillance and corruption. The Committee stressed that more should be done in relation to beneficial ownership registries, which lack transparency although they were designed to shed light on such information.

76. 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 with both eavesdropping techniques and spyware by the Cypriot government since February 2018^{1a} (581, 579). Cyprus is an important European export hub for the surveillance industry. 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 at 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.

76 a (new). There are close connections between Cyprus and Greece when it comes to the topic of spyware. Tal Dilian's Intellexa is established in Greece and his spyware Predator has been used in the Greek hacking scandals (577, 578). Both countries were also involved in the illegal export of Predator spyware to the Sudanese Rapid Support Forces (RSF) militias^{1a} (577). Greece has issued an export licence, whereas the material was transported to Sudan from Larnaca airport^{1b}.

Footnotes:

1a. LightHouse Reports. Flight of the Predator.

1b. <https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/>

76 b (new). Next to the export of spyware outside the EU, Cyprus also facilitates the trade of subsystems and spyware technology to Member States. UTX Technologies - registered in Cyprus and acquired by the Israeli technology giant Verint - has been spotted on invoices with German, French and Polish companies for the shipping of Gi2 technology and monitoring systems^{1a} (580).

Footnote:

1a Philenews. Cyprus is a pioneer in software exports (documents)

77. 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 stipulating the use of interception devices and the protection of constitutional rights of citizens.

COMP 73 (Paragraph 78 - 78 c (new))

*Covered: AM 586 (Rapporteur), AM 587 (Greens), AM 588 (Rapporteur), AM 589 (Greens), AM 590 (Rapporteur), AM 591 (Greens), AM 595 (S&D), AM 598 (S&D),
Fall: AM 583 (EPP), AM 584 (Mandl), AM 585 (ECR)*

Legal Framework

Dual-Use Regulation

78. Cyprus seems to have a very close collaboration with Israel in the area of surveillance technologies. Cyprus consulted with Israel and the US about the reform of its legal framework *and system of control of exports of dual-use items*. Cyprus is a popular destination for many Israeli spyware companies.

78 a (new). *The Ministry of Energy, Commerce and Industry in the Strategic Items Export Licensing Section regulates the export of dual use items^{1a}. In response to the PEGA questionnaire that was sent to all Member States, Cyprus stated that it monitors and assesses all export license applications for dual-use goods on a case-by-case basis, in full accordance with relevant sanctions regimes. These regimes are the European Union Global Human Rights Sanctions Regime, as well as the EU Regulation for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items [Regulation (EU) 2021/821], guided by the criteria of the relevant Council Common Position (2008/944/CFSP)^{1b} (586, 587). The PEGA committee observes that Cyprus is not a signatory of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. It was stated that Turkey blocked Cypriot membership to this agreement during the PEGA committee mission (598). However, the government declares it is adhering to the same standards (586,587).*

Footnotes:

1a http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument

1b Reply to European Parliament questionnaire received from Cyprus.

78 b (new). *The Ministry of Energy, Commerce and Industry can consult the so-called Advisory Committee when it comes to permitting an export license. This committee consists of representatives from the Ministry of Defence, Ministry of Justice and Public Order, Ministry of Foreign Affairs, the Customs and Excise Department amongst other departments^{1a}. 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 of this committee^{1b}. The Chamber of Commerce usually does not provide information on the number of approved and rejected software-marketing licenses^{1c} (588, 589).*

Footnotes:

1a Lelaw. Export Controls for dual-use products.

1b Reply to European Parliament questionnaire received from Cyprus.

1c Inside Story. Who signs the exports of spyware from Greece and Cyprus?

78 c (new). *During the PEGA committee's mission to Cyprus on 1 and 2 November 2022, the participants to the mission had a meeting with the Ministry for Energy, Commerce and Industry (595). Ministers Natasa Pilides and Kyriacos Kokkinos stated that there has been a sharp decline in the number of companies active in Cyprus. 32 companies are registered, but according to the Minister currently only 8-10 are active of which 3-4 produce spyware^{1a} (590, 591). However, they also admitted to technical challenges in overseeing and controlling companies based in Cyprus selling individual components of spyware independently (595).*

Footnote:

1a 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 02.11.2022

COMP 73 (Paragraph 79 - 79 h (new))

Covered: AM 592 (Rapporteur), AM 593 (Rapporteur), AM 594 (S&D), AM 596 (Rapporteur), AM 597 (Rapporteur), AM 599 (Rapporteur), AM 600 (Rapporteur), AM 601 (Rapporteur), AM 602 (Rapporteur), AM 625 (Left)

Fall:

79. In practice, (592) ~~Compared to its legal framework in place~~ Cyprus is reportedly rather lenient in providing spyware companies with export licenses¹³⁷. Companies use ~~tricks~~ **techniques** to circumvent the rules. That is, the physical hardware of the product is sent to a recipient country without the software loaded on it¹³⁸. After that, the activation software (also referred to as the 'license key') is sent separately by means of an usb-memory stick to the destination country¹³⁹. Another way is to state that the product is exported for demonstration purposes only, although a detailed description of the product is added¹⁴⁰. **In addition, unclear description of spyware in the export form linked to the export licence hindered appropriate custom checks (594).**

Footnotes:

137 InsideStory. Who signs the exports of spyware from Greece and Cyprus? <https://insidestory.gr/article/oi-exagoges-spyware-apo-ellada-kai-kypro>

138 InsideStory. Who signs the exports of spyware from Greece and Cyprus? <https://insidestory.gr/article/oi-exagoges-spyware-apo-ellada-kai-kypro>

139 <https://www.philenews.com/eidiseis/politiki/article/1552708>

140 <https://www.philenews.com/koinonia/eidiseis/article/1549262>

79 a (new). *Several Cypriot companies have reportedly obtained export licenses for the sale of 'dual use items' to third countries. These companies are UTX Technologies, Coralco Tech, Prelysis and Passitora^{1a} (593).*

Footnote:

1a Philenews. Cyprus is a pioneer in software exports (documents); Haaretz. Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record.

79 b (new). *UTX Technologies has been involved in the sale of spyware to EU Member States as well as to third 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^{1a} (596).*

Footnote:

1a Philenews. Cyprus is a pioneer in software exports (documents)

79 c (new). *The Cypriot trade agency 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^{1a}. UTX Technologies reportedly also had a contract with Thailand for the sale of surveillance subsystems for 3 million dollars. The description of this subsystem 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 license, the Ministry of Energy, Commerce and Industry could be circumvented through the Lithuanian registered UAB Communication Technologies^{1b}. Russian-Israeli citizen Anatoly Hurgin owns this company and in addition holds a Maltese passport^{1c}. In addition, UTX also secured an agreement with Bangladesh for a Web Intelligence System for 2 million dollars in 2019 and for a cellular tracking system for 500.000 dollar in 2021^{1d} (597).*

Footnotes:

1a Philenews. Cyprus is a pioneer in software exports (documents)

1b Philenews. Cyprus is a pioneer in software exports (documents)

1c https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/

1d Haaretz. Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record.

79 d (new). *Cyprus’ export history also shows that Coralco Tech - originally from Singapore but also registered in Israel and Nicosia - shipped monitoring equipment for 1.6 million dollars to the Bangladeshi military after a tender process in 2018. The owner of Coralco Tech is the Israeli Eyal Almog^{1a} (599).*

Footnote:

1a Haaretz. Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record.

79 e (new). *In 2019, the internal intelligence agency of Bangladesh (NSI) bought a Wi-Fi interception software from Prelysis registered in Cyprus for a total of 3 million dollars. Kobi Naveh - the founder and director of Prelysis - used to work for the Israeli company Verint until 2014^{1a}. Verint is also the company that acquired the in Cyprus registered UTX Technologies (600).*

Footnote:

1a Haaretz. Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record.

79 f (new). *In summer 2021, Bangladesh additionally bought a spy vehicle from Tal Dilian’s firm Passitora (that used be to known as WiSpear). The Swiss company Toru Group Limited, as registered on the British Virgin Islands, served as an intermediary for the agreements made with Dilian’s Passitora^{1a} (601).*

Footnote:

1a Haaretz. Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record.

79 g (new). *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^{1a}. According to media reports and statements made by the DISY 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 (625).^{1b} It is not clear whether or not the contract was signed and any spyware was provided to the Dutch Defence Ministry.*

Footnote:

1a 251 <https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/>

1b <https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/>

79 h (new). *These examples show there is a lot of activity of the surveillance industry on Cyprus, involving the same actors that emerge in the spyware scandal that is being investigated by PEGA (602).*

COMP 75 (Paragraph 80)

Covered: AM 567 (Rapporteur), AM 603 (Rapporteur)

Fall: AM 604 (Mandl), AM 605 (EPP)

80. Many Israeli companies come to Cyprus to start off their European activity¹⁴¹. Different sources reported furthermore that the country is home to approximately 29 Israeli companies¹⁴². ***Some sources point to a close connection between the trade in spyware and diplomatic relations are closely connected.*** In return for the facilitation of licenses for Israeli companies, Cyprus has allegedly received some of the products these companies develop and export, like the Pegasus spyware from NSO¹⁴³ as well as spyware materials from WiSpear¹⁴⁴. ***Cyprus serves as the foothold in the trade of Israeli spyware within the EU's internal market as well as the export of spyware to third countries (567, 603).***

Footnotes:

141 Philenews. *Revelations in Greece: Predator came from Cyprus*

142 Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022

143 Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

144 Inside Story. *Predator: The 'spy' who came from Cyprus*.

COMP 76 (Paragraph 81 - 81 b (new))

Covered: AM 606 (Rapporteur), AM 607 (Greens), AM 608 (Rapporteur), AM 609 (Rapporteur), AM 610 (Greens), AM 611 (Greens)

Fall:

Ex-ante

scrutiny

81. The law on the Protection of the Confidentiality of Private Communications 92(I)/1996 stipulates that the ***Attorney General may submit an application for authorisation to monitor 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 happens upon a written request by the Chief of Police, the Commander of the Cyprus Intelligence Service or an investigative judge. Provisions on the authorization or approval can however be overruled in cases where the interception of private communication must be submitted to the Court¹⁴⁵ is in the security interests of Cyprus, or to prevent, inquire or prosecute offences¹⁴⁵ (606, 607).***

Footnote:

145 CyLaw. *The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996)*

81 a (new). *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 authorisation to employees of their service, or employees carrying out assignments for their service, to intercept private communication and/or get access to the monitoring equipment for the sake of technical work^{1a} (608, 610).*

Footnote:

1a CyLaw. *The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996)*

81 b (new). *In addition, article 4(2) of Law 92(I)/1996 as amended in 2020^{1a}, 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 up to a fine of 50 000 euro and/or up to 5 years imprisonment^{1b}. 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 also not apply to the surveillance systems used by the Chief of the Police and the Commander of the KYP^{1c} (609, 611).*

Footnotes:

1a CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020

1b Reply to European Parliament questionnaire received from Cyprus.

1c Reply to European Parliament questionnaire received from Cyprus.

COMP 77 (Paragraph -82 a (new) to Paragraph -82 b (new))

Covered: AM 612 (Rapporteur), AM 613 (Greens), AM 614 (Rapporteur), AM 615 (Greens), Fall:

Ex-post scrutiny

-82 a (new). *In Cyprus, the Processing of Personal Data (protection of individuals) law from 2001 outlines 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^{1a}. This right can be circumvented once the Commissioner for the Protection of Personal Data decides otherwise in light of national security reasons amongst others^{1b}. (612, 613).*

Footnotes:

1a CyLaw. *The Processing of Personal Data (Protection of Individuals) Law of 2001 (138(I)/2001).*

1b Franet EU. *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies. Legal update.*

-82 b (new). *Moreover, the Protection of the Confidentiality of Private Communication Law as agreed on in 1996, spells out that in case of interception of private communications by law enforcement agencies, the Attorney General is obliged to inform the individual in question. Notifying the individual must occur within a maximum period of 90 days from the start of the issuance of the judicial warrant^{1a}, 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 fact of the issuance of the court warrant, the date of the issuance of the court warrant and the fact that within this period, interception or access to*

private communications has occurred. This obligation can be delayed if the Attorney General decides that withholding this information is in the interest of the security of Cyprus, amongst others^{1b}. The Court can also order for non-disclosure of the information in light of security interests of Cyprus^{1c}.(614, 615)

Footnotes:

1a CyLaw. Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).

1b Franet EU. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies. Legal update.

1c CyLaw. Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).

COMP 78 (Paragraph 82)

Covered: AM 616 (ID), AM 617 (Rapporteur),

Fall:

82. ~~On paper,~~ Violating (616) the protection of private communications is a de jure criminal offense. De facto, this illegality is often hidden behind the invocation of national security¹⁴⁶. There is no ~~legislature~~ **legislation (617)** covering how the Police or other intelligence services use the interception devices, who regulates the procedures of interception and how the protection of constitutions rights of citizens is guaranteed. The relevant regulations and protocols are currently pending in the House of Representatives for discussion and approval. For the time being, these provisions remain unchecked¹⁴⁷.

Footnotes:

146 Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.

147 Philenews. Legal but uncontrolled interceptions.

COMP 79 (Paragraph -83 a (new) to Paragraph -83 b (new))

*Covered: AM 618 (Rapporteur), AM 619 (Greens), AM 620 (Rapporteur), AM 621 (Greens),
AM 622 (Left)*

Fall:

Redress

-83 a (new). *The legality of the actions of the Cyprus Intelligence service are evaluated by a three-member committee as outlined in the Cyprus Intelligence Service Law 74(I)/2016. The tripartite committee is appointed by the Council of ministers, following a recommendation by the President of the Republic^{1a} (618, 619, 622).*

Footnote:

1a Reply to European Parliament questionnaire received from Cyprus.

-83 b (new). *The law of 92(I)/1996 was amended in 2020 and strengthened the oversight framework of the Republic, in particular the provisions concerning the tripartite committee. In the remit of its mandate, the committee can initiate ex officio inquiries and can start investigations into the facilities, technical equipment and archived material from the KYP. As introduced by the Article 17A(1) of Law 92(I)/1996 as amended by Law 13(I)/2020, the*

committee can also start inquiries into the Police' facilities, technical equipment and archived material. In light of such investigations, the committee can appeal 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 provides the President of the Republic with an annual report, in which it outlines the activities, formulates observations and recommendations and identifies omissions^{1a} (620, 621).

Footnote:

1a Reply to European Parliament questionnaire received from Cyprus; CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020

COMP 80 (Paragraph 83)

Covered: AM 623 (Rapporteur), AM 624 (Greens)

Fall:

83. The President of Cyprus has a significant say in the formation of the committee that is capable of starting critical inquiries in the actions of the KYP. In addition, the annual reports with the committee's findings are first sent out to the President¹⁴⁸. ***At the time of writing, there is no information on the exact composition of the committee, its work and the scrutiny it performs^{148a} (623, 624).***

Footnotes:

148 Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

148a Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

COMP 81 (Paragraph 84 to Paragraph 86)

Covered: AM 627 (Rapporteur) , AM 628 (Rapporteur), AM 629 (Greens)

Fall: AM 626 (S&D),

Key figures in the spyware industry

84. Tal Dilian has played a key role in many of the developments that took place in Cyprus and Greece. He obtained Maltese citizenship in 2017¹⁴⁹ Tal Dilian served in different leadership positions in the Israeli Defence Force for 25 years before he retired from the military in 2002¹⁵⁰ Starting off a career as “intelligence expert, community builder and serial entrepreneur” in Cyprus, Dilian launched Aveledo Ltd., later to be known as Ws WiSpear Systems Ltd. and after that Passitora Ltd¹⁵¹.

Footnotes:

149 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>

150 <https://taldilian.com/about/>

151 Opencorporates. Passitora ltd

85. In Cyprus, Dilian became closely associated with Abraham Sahak Avni. Avni has formerly been involved in the Israeli Police Special Forces as special detective¹⁵². In November 2015, he acquired Cypriot citizenship and a golden passport because of a 2.9 million euro investment in real estate¹⁵³. Avni founded the Cypriot NCIS Intelligence Services Ltd¹⁵⁴, a company that

was reportedly involved with the most powerful technology-oriented companies in the world¹⁵⁵. NCIS Intelligence and Security Services provided security software to the Police Headquarters between 2014 and 2015 and instructed employees of the Office of Crime Analysis and Statistics between 2015 and 2016¹⁵⁶. Government Party DISY (Dimokratikós Sinagermós) is also part of the company's clientele. Reportedly, Avni had installed security equipment in the party's offices¹⁵⁷. Next to Avni's security equipment, Dilian's materials were also sold to the Cyprus Drug Enforcement Agency and the Cypriot Police¹⁵⁸.

Footnotes:

152 ShahakAvni. *About Shahak Avni.*

153 Report by Fanis Makridis. *PEGA Mission to Cyprus on 01.11.2022*

154 Philenews. *ΦΑΚΕΛΟΣ: Η Πολιτεία υπέθαλπε Άβνι και Ντίλιαν*

155 Report by Fanis Makridis. *PEGA Mission to Cyprus on 01.11.2022.*

156 Philenews. *ΦΑΚΕΛΟΣ: Η Πολιτεία υπέθαλπε Άβνι και Ντίλιαν*

157 Tovima. *The unknown "bridge" between Greece and Cyprus for the eavesdropping system.*

158 Inside Story. *Predator: The "spy" who came from Cyprus.*

85 a (new). At one point, the Headquarters Crime Investigation Department of the Police found violations of the confidentiality of private communications related to Avni's company. The police decided to close the case^{1a} (628, 629).

Footnote:

1a Report by Fanis Makridis. *PEGA Mission to Cyprus on 01.11.2022.*

86. The connections between Dilian and Avni are numerous. Dilian's company WiSpear shared a building in Lacarna and some of its personnel with Avni¹⁵⁹. In 2018, the two men launched Poltrex company, which is later renamed to Alchemycorp Ltd. Poltrex is hosted in the Novel Tower as shared with Avni and is also part of Intellexa Alliance. Reportedly, Avni's relations with the DISY party created the testing ground for Dilian's products¹⁶¹.

Footnote:

159. Report by Fanis Makridis. *PEGA Mission to Cyprus on 01.11.2022.*

160 CyprusMail. *Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.*

161 Inside Story. *Predator: The "spy" who came from Cyprus.*

COMP 82 (Paragraph 87 - 87 b (new))

Covered: AM 569 (Rapporteur), AM 570 (Greens), AM 571 (Rapporteur), AM 572 (Greens), AM 630 (Rapporteur), AM 631 (Greens), AM 632 (rapporteur), AM 633 (Greens),

Fall:

Dilian's spyware van

87. After the sale of Circles technologies and the founding of WiSpear, Tal Dilian additionally launched Intellexa Alliance in 2019, described on the website as an 'EU based and regulated company with the purpose to develop and integrate technologies to empower intelligence agencies'.¹⁶² There are different surveillance vendors that fall under the marketing label of Intellexa Alliance, like Cytrox, WiSpear - later renamed under Passitora Ltd. - Nexa technologies and Poltrex ltd. These different vendors under Dilian's alliance allow for a broad assortment of surveillance software and services that Intellexa can offer and combine to its clients.¹⁶³ More detailed information on the corporate structure **can be found** in the chapter on the Spyware Industry.

Footnotes:

162 <https://intellexa.com/>

163 Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*

87 a (new). *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 9 million euro worth van was capable of hacking devices within a range of 500 meters^{1a}. The public attention generated by the Forbes interview^{1b} 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 included Larnaca International Airport^{1c} (569, 570, 630, 631).*

Footnotes:

1a Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.*

1b Forbes. *A Multimillionaire Surveillance Dealer Steps Out Of The Shadows ... And His \$9 Million Whatsapp Hacking Van.*

1c Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.*

87 b (new). *On June 16 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, whereafter three WiFi antennas were installed^{1a}. Although not registered in Cyprus, Israeli company Go Networks was also involved in the negotiations leading up to the arrangement^{1b}. The true reason for the agreement was however to test WiSpear's interception technology. The intercepted data of passengers was saved in the airport server room, close in proximity to the WiSpear office in Larnaca as shared with Avni^{1c}. During the period of time when the antennas were operable, intercepted data was retrieved from 9.507.429 mobile devices^{1d} (571, 572, 632, 633).*

Footnotes:

1a Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.*

1b Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

1c Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

1d Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

COMP 83 (Paragraph 88 to Paragraph 88 c (new))

*Covered: AM 573 (Greens), AM 574 (Rapporteur), AM 575 (Rapporteur), AM 576 (Greens), AM 634 (Rapporteur), AM 635 (Greens), AM 636 (Rapporteur), AM 637 (Greens), AM 638 (Rapporteur), AM 639 (Greens), AM 640 (Rapporteur), AM 641 (Greens),
Fall: /*

88. Following the complaints against Dilian, ~~it became clear that the~~ 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 provided with top ~~functions~~ **positions** at Intellexa¹⁶⁴. In addition, the police investigations found that export licenses had been granted to WiSpear for 'Interception equipment designed for the extraction of voice or data, transmitted over the air interface'^{165 166}. ***Dilian's companies, as stated by the Chamber of Commerce, have not received any export licenses in the last two years. At time of writing, it remains unclear who authorised these export licenses^{166a}. (634, 635).***

Footnotes:

164 Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.*

165 Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

166 Philenews. *Export of tracking software from Cyprus.*

166a Inside Story. *Who signs the exports of spyware from Greece and Cyprus?*

88 a (new). *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^{1a}. 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 (636, 637).*

Footnote:

1a Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022

88 b (new). *On 15 November 2021, the case was brought before the Criminal Courts with WS WiSpear Systems ltd, Tal Dilian and two other WiSpear employees as defendants. Ultimately, Attorney General George Savvides upheld the case against the company WiSpear, but the criminal proceedings against Dilian and the employees were dropped^{1a}. The reasons for that decision are classified. However, the Attorney General could decide at any given moment to reopen the case against the three individuals (638, 639).*

Footnote:

1a Financial Mirror. *Anger after 'spy van' charges dropped.*

88 c (new). *WiSpear pleaded guilty to 42 charges and was fined with 76000 euros in the Assize court on 22 February 2022^{1a}. WiSpear confessed to charges of illegal surveillance of private communications and data protection violations^{1b}. The Court published its final decision, 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 emphasized that no damage was caused to any individual person"^{1c}. In addition to a fine imposed by the Assize court, Commissioner for Personal Data Protection Irini Loizidou Nicolaidou fined WiSpear with 925,000 euro in light of GDPR violations^{1d}(640, 641). Although it was asserted that the episode with the Black Van touches upon matters of national interest and critical infrastructure, the sanctions for the perpetrators were very light (575, 576). This incident may have political significance beyond the violation of the privacy of passengers. Given that Cyprus is situated on a cross-roads in many ways, there are several third countries that could potentially have an interest in having insight into the traveller movements through Larnaca airport: Turkey, Israel, Russia and the US, for example. (573, 574)*

Footnotes:

1a Makarios Drousiotis. *Κράτος Μαφία*.. Chapter 6. Published 2022; Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022

1b Financial Mirror. *Spy van company fined €76,000.*

1c Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.*

1d CyprusMail. *Israeli company that deployed 'spy van' fined €925,000 for data violations; Financial Mirror. Spy van company fined €76,000.*

COMP 84 (Paragraph 89 to Paragraph 90)

Covered: AM 644 (Left)

Fall:

~~89. In 2011, 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 2011¹⁶⁷ and was registered with the assistance of the former law firm of Savvas Angelides¹⁶⁸. Their partnership however dissolved in 2012. Nevertheless, Savvas Angelides was the person in charge of Avni and Dillian in the case of the surveillance van¹⁶⁹.~~

Footnotes:

~~167 Politis. "Interceptions" file: Classified Police Report (2016) shows he knew everything about Avni~~

~~168 Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022.~~

~~169 Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.~~

90. Opposition party AKEL expressed outrage over the cases against Dilian and staff being dropped, and denounced the legal decision as a cover-up by the Attorney General¹⁷⁰. After all, the Cypriot government had reportedly purchased equipment from Dilian's company and one of the accused employees had allegedly worked for NSO, providing the KYP with instructions on how to use the Pegasus spyware¹⁷¹. Dropping the charges ensured that the information on the links between Dilian's company and the Cypriot government would remain protected¹⁷². ***The Attorney General has refused to hand over the conclusions of the investigation, even though it was requested during the official mission by the PEGA Committee in Cyprus (644).*** This example shows that the violation of data protection rights of individuals by mass surveillance equipment is not fully guaranteed. Whilst legal remedy exists on paper, judicial outcomes ***are could be*** influenced by governmental interventions, leaving the individual victim defenceless. ***The investigation furthermore displayed that Cyprus has become a ground for the experimentation of surveillance equipment by the Cypriot based companies themselves.***

Footnotes:

170 Financial Mirror. Anger after 'spy van' charges dropped.Le

171 Makarios Drousiotis. *Κράτος Μαφία..* Chapter 6. Published 2022.

172 Makarios Drousiotis. *Κράτος Μαφία..* Chapter 6. Published 2022.

COMP 85 (Paragraph 91)

Covered: AM 645 (Rapporteur), AM 646 (Greens),

Fall: /

The move to Greece

91. Following the episode of the van and the lawsuit, Dilian moved Intellexa's operations to Greece. Although he never left Cyprus, ~~and is still a resident~~ ***he is reportedly planning his return to Tel Aviv^{1a}(645).*** Indirect links between several natural and legal persons as registered in Cyprus and Greece expose the facilitation of Dilian's businesses to Athens¹⁷³. ***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 (645, 646).***

Footnotes:

1a Intelligence Online. Israeli cyber tsar Tal Dilian plans Tel Aviv return.

173 Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.

COMP 86 (Paragraph 92 to Paragraph 92 a (new))

Covered: AM 647 (EPP)

Fall: AM 648 (Rapporteur), AM 649 (Left), AM 650 (Rapporteur), AM 651 (Greens)

~~92. According to recent testimonies in light of the judicial investigations in the van case, lawyer Aleksandros Sinka has had significant influence in the move to Greece. Sinka—who formerly played a key role in the centre-right DISY party—apparently had good relations with both Dilian and Avni¹⁷⁴. It appears that Sinka was also an acquaintance of former General Secretary of the Greek government Dimitriadis. Both men held positions in the Bureau of the European Democrat Students (EDS), the student organisation of the European People's Party (EPP). Between 2003 and 2004, Sinka served as Chairman and Dimitriadis as Vice Chairman¹⁷⁵. Dimitriadis allegedly introduced his friend and Greek businessperson Felix Bitzios to Sinka, in view of Bitzios' long-standing dispute in the Cypriot court. Sinka in turn recommended lawyer Harris Kyriakidis to help Bitzios in his dispute. Kyriakidis equally had good relations with the DISY¹⁷⁶.~~

Footnotes:

~~174 Tovima. The unknown “bridge” between Greece and Cyprus for the eavesdropping system.~~

~~175 EDS. 2003/2004 Bureau.~~

~~176 Tovima. The unknown “bridge” between Greece and Cyprus for the eavesdropping system.~~

92 a (new). The judicial investigations led to the transfer of Avni's and Dilian's activities in Poltrex to Yaron Levgoren. 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^{1a}. According to his LinkedIn he currently represents the in Greek-based Intellexa company Apollo Technologies (650, 651).

Footnote:

1a Philenews. How the spyware scandal in Greece is related to Cyprus.

COMP 87 (Paragraph 93 to Paragraph 94)

Covered: AM 652 (Rapporteur), AM 653 (Greens), AM 654 (Rapporteur), AM 655 (Greens),

Fall:

NSO Group Spyware companies and Cyprus

93. Next 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 vulnerabilities¹⁷⁷. Six years later, Circles Technologies was sold to Francisco Partners for just under 130 million dollars of which 21.5 million dollars went to 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 March 29, 2016¹⁷⁸.

Footnotes:

177 Amnesty International. Operating from the Shadows.

178 Amnesty International. Operating from the Shadows.

93 a (new). 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, nor officially exported from Cyprus^{1a} (652, 653).

Footnote:

1a Reply to European Parliament questionnaire received from Cyprus.

93 b (new). *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 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.”^{1a} (654, 655).*

Footnote:

1a Amnesty International. Operating from the Shadows.

~~94. The denial by the Cypriot government of the Pegasus export and development in the country seems however incorrect.~~ **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 are engaged in software providing intelligence services¹⁷⁹. 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 ~~seems to have~~ **reportedly** issued an invoice of 7 million dollars for services to the company in question¹⁸⁰. **This information cannot however be confirmed.**

Footnotes:

179 Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

180 Akel report. PEGA mission to Cyprus.

COMP 88 (Paragraph 95 to Paragraph 95 d (new))

Covered: AM 642 (Rapporteur), AM 643 (Greens), AM 656 (Rapporteur), AM 657 (Rapporteur), AM 658 (Greens),

Fall: /

95. Reportedly, NSO Group also had an active company in Cyprus that allegedly hosted a customer service center. 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 an amount of €55 million^{181 182}. It should be noted here that a year later, on 2 October 2018, the Saudi regime killed Jamal Khashoggi in the Saudi consulate in Turkey, after ~~surveilling~~ **surveilling** him and his near ones with Pegasus (656). **This is disputed by NSO.**

Footnotes:

181 Makarios Drousiotis. *Κράτος Μαφία.. Chapter 6*. Published 2022.

182 Haaretz. *Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals*.

95 a (new). *According to CitizenLab, 25 state actors were clients of Circles Technologies in 2020. Amongst these state actors were Belgium, Denmark, Estonia and Serbia^{1a}. As of 2020, NSO Group has closed their Circles office stationed in Cyprus. At the time of writing, it remains unclear which Circles' companies remain operable^{1b} (657, 658).*

Footnotes:

1a CitizenLab. *Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles*

1b Amnesty International. *Operating from the Shadows*.

95 b (new). *The Israeli QuaDream is an additional 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^{1a}. Through InReach, a Cyprus registered company since 2017, QuaDream products were indirectly sold to customers and thus circumvented Israeli export controls. The two companies are in an ongoing legal dispute^{1b}.*

Footnotes:

1a <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-adeb-ebdc048c0000>

1b <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/>

95 c (new). *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 current Deputy Attorney General Savvas Angelides^{1a}. Angelides sold his shares in A.I.L. Nominee Services to Christos Ioannides on February 16 2018, a few weeks before he became Minister of Defence^{1b}. However, A.I.L. Nominee Services remains the director and secretary of InReach^{1c} and thus in business with a company exporting QuaDream products to third countries.*

Footnotes:

1a <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/> ; <https://opencorporates.com/companies/cy/HE373827>

1b <https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/>

1c <https://opencorporates.com/companies/cy/HE373827>

95 d (new). *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^{1a}, with the assistance of the former law firm of Savvas Angelides^{1b}. 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^{1c}. The partnership between Michael Angelides and Avni was however dissolved in 2012. Savvas Angelides became Deputy Attorney General in 2020 and was the person in charge of investigating Avni and Dillian in the case of the surveillance van^{1d}. In a press statement on 10 August 2022, the Deputy Attorney General declared that he nor his relatives had any connection with Tal Dillian. On the partnership between Michael Angelides and Avni, he mentions 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"^{1e} (642, 643). 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^{lf}, nor on the role of the company as secretary in the partnership between his relative and Avni in S9S.

Footnotes:

1a Politis. "Interceptions" file: Classified Police Report (2016) shows he knew everything about Avni

1b Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022.

1c <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>

1d Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

1e Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022.

1f

<https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=271194&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1>

COMP 89 (Paragraph 96)

Black Cube

Covered: AM 659 (Rapporteur), AM 660 (Greens),

Fall: /

96. Black Cube is a company employing former officers of Israeli Intelligence Agencies, like 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 Cyprus¹⁸³. ***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 involvement of Black Cube" since the lawsuit "came from nowhere and I want to understand"***^{183a}. ***Black Cube was also exposed in spying scandals in Hungary and Romania. (659, 660).***

Footnotes:

183 The New Yorker. How Democracies Spy on their Citizens.

183a The New Yorker. How Democracies Spy on their Citizens.

COMP 90 (Paragraph 97 to Paragraph 97 d (new))

Covered: AM 661 (Rapporteur), AM 662 (Greens), AM 663 (Rapporteur), AM 664 (Greens), AM 665 (Rapporteur), AM 666 (Greens), AM 667 (Rapporteur), AM 668 (Greens),

Fall: /

Purchase and use of Spyware by Cyprus

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

97 a (new). *After the elections of 2013, Andreas Pentaras was appointed as head of the Cyprus Intelligence Service whilst surveillance expert Andreas Mikellis was responsible for the protection of President Anastasiades' communications. In that same year, 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^{1a}. The DaVinci software was able to infect applications of a mobile phone and therefore did not meet the official requirements for the lifting of privacy^{1b} (661, 662).*

Footnotes:

1a Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

1b Inside Story. Predator: The "spy" who came from Cyprus.

97 b (new). *Disclosed contact information as revealed by WikiLeaks between Mikellis and Hacking Team indicated the bypassing of tender procedures and lack of proper review of the acquired surveillance system. At the start of 2014, the software was reportedly installed and four employees of the KYP were trained, including Mikellis^{1a} (663, 664).*

Footnote:

1a Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

97 c (new). *When WikiLeaks revealed the purchase of Hacking Teams' surveillance software, the KYP confirmed that this system was used for national purposes only^{1a}. Despite Mikellis contact with Hacking Team^{1b}, it was the head of the KYP Andreas Pentaras who ultimately resigned after these revelations came to light^{1c}. Kyriakos Kouros replaced Pentaras (665, 666).*

Footnotes:

1a Inside Story. Predator: The "spy" who came from Cyprus.

1b Makarios Drousiotis. *Κράτος Μαφία*. Chapter 6. Published 2022.

1c CyprusMail. Intelligence chief resigns after spy tech revelations. <https://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/>

97 d (new). *According to WikiLeaks, one more 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^{1a} (667, 668). It is however unclear which police department is at issue here (667).*

Footnote:

1a Inside Story. Predator: The "spy" who came from Cyprus.

COMP 91 (Paragraph 98 to Paragraph 98 d (new))

~~Victim~~ Target Makarios Drousiotis

Covered: AM 669 (S&D), AM 670 (Rapporteur), AM 671 (Greens), AM 672 (Rapporteur), AM 673 (Greens), AM 674 (Rapporteur), AM 675 (Greens), AM 676 (Rapporteur), AM 677 (Greens),

Fall:

98. Starting at February 2018, investigate journalist Makarios Drousiotis was allegedly spied on by the Cypriot government **with both eavesdropping techniques and spyware^{1a}**. This case of espionage started during Drousiotis former function as 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 Drousiotis, it was his latter role that triggered the first surveillance attempt.¹⁸⁴

Footnote:

1a <https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/>

184 Makarios Drousiotis. *Κράτος Μαφία*. Chapter 5. Published 2022

98 a (new). *In the course of 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 the sake of communication interception of the British Foreign Office computer systems^{1a}. At this point, 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^{1b}. In light of these events, Drousiotis believes the Cypriot government - more particularly the Cyprus Intelligence Service - to be behind the infection of his phone (670, 671).*

Footnotes:

1a BBC. No 10 network targeted with spyware, says group.

1b Makarios Drousiotis. *Κράτος Μαφία*. Chapter 5. Published 2022.

98 b (new). *In May 2019, Drousiotis sent a letter to President Anastasiades expressing his concerns around the surveillance of his phone, outlining the potential motives behind this surveillance as well as holding the President personally accountable for whatever may happen to him after the espionage. Anastasiades forwarded the letter to the current head of the Cyprus Intelligence Service Kyriakos Kouros. Both Anastasiades and Kouros have refuted the alleged surveillance with the Pegasus software, reiterating that NSO Group was in fact not even registered in Cyprus^{1a} (672, 673).*

Footnote:

1a Makarios Drousiotis. *Κράτος Μαφία*. Chapter 5. Published 2022.

98 c (new). *In the months that followed, several intimidation attempts occurred including the disappearance of evidence on his computer, the disconnection of security cameras at Drousiotis home and being tracked by strangers. After going public with his story and submitting a complaint at the Cypriot police office, Drousiotis got in touch with Lambros Katsonis, Head of the Technical Support Department of Panda Security, a Cypriot company specialised in antivirus equipment. Drousiotis was however unaware of the fact that the Cypriot government also used this antivirus software for their own devices. Against this background, Katsonis seems to have been sent to Drousiotis home under false pretences. Possibly with the aim to further infiltrate Drousiotis devices as instructed by the Cypriot Intelligence Service (KYP)^{1a} (674, 675).*

Footnote:

1a Makarios Drousiotis. *Κράτος Μαφία*. Chapter 5. Published 2022.

98 d (new). *As of spring 2019, Drousiotis became aware of the suspicious entries in his Android phone and reached out to Google One Support to confirm the nature of these entries. Yet, Google does in general not respond to surveillance related matters, referring the customer in question to the national law enforcement agencies^{1a}. Mr Drousiotis, though not*

having any confidence in the police, did agree to hand over his devices for forensic examination (676, 677).

Footnote:

Ia Makarios Drousiotis. Κράτος Μαφία. Chapter 5. Published 2022.

COMP 92 (Paragraph 99)

Covered:

Fall: AM 678 (EPP), AM 679 (Mandl), AM 680 (ECR)

Concluding remarks

99. Cyprus ~~appears to have~~ **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 politics, 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 the 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 the trade in spyware. Export licenses for spyware have become a currency in diplomatic relations.

Compromises on Spain

COMP 93 (Paragraph 100 -a (new) to Paragraph 100 b (new))

Covered: AM 879 (S&D), 890 (S&D)

Fall:

I.E Spain

100 -a (new). Following the invitation by the PEGA Committee in the European Parliament, 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 (AM 879). Due to these stated “legal constraints”, the answers in front of the Committee were limited and left most questions open.

100 -b (new). 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 with 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.

Paragraph 100

Covered: 682 (EPP), 683 (EPP), 684 (S&D), 688 (Left), 689 (Cañas), 690 (EPP), 695 (Cañas)

Fall: 681 (Cañas), 685 (ECR), 686 (Puigdemont), 687 (ID)

100. 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. ~~It is widely believed that the Moroccan authorities targeted~~ *In May 2022, a report in The Guardian newspaper identified Morocco as possibly having spied on more than 200 Spanish mobile phones (AM 689). The Spanish government confirmed that* Prime Minister Pedro Sanchez, Minister ~~for~~ *of* Defence Margarita Robles and Minister of the Interior Fernando Grande-Marlaska; ~~similarly to the case of the French President and government ministers¹⁸⁵~~ *have been infected by Pegasus spyware, while Minister of Agriculture Luis Planas was targeted but not infected^{185a} (AM 682). 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 (AM 689).* The targeting of a second group of ~~victims~~ *targets* is referred to as 'CatalanGate'¹⁸⁶. It includes Catalan parliamentarians, Members of the European Parliament, lawyers, *journalists (AM 684)*, civil society organisation members, *academics (AM 688)* and some family and staff connected to those victims¹⁸⁷, *which can be referred to as 'indirect' or 'relational' targeting.* The 'CatalanGate' surveillance case was first reported on in 2020, *after a joint investigation by the Guardian and El País^{187a}*, but it was not until April 2022 that Citizen Lab completed their in-depth investigation that the scale of the case was revealed. The results of that probe showed that at least 65 persons were targeted¹⁸⁸. *It should be noted that as of December 2022 Citizen Lab acknowledged that one infection was incorrectly attributed due to an error in labelling of initials^{188a}, although the overall number of Catalan targets remained unchanged (AM 690).* In May 2020 ~~2022~~, the Spanish authorities admitted to targeting 18 ~~individuals of those 65 victims~~ *with court authorisation¹⁸⁹, although the warrants for those cases are not disclosed. The former director of the CNI Paz Esteban appeared before the Official Secrets Committee of the Parliament held in camera, to provide justification for the surveillance of these 18 persons (AM 683).*

Footnotes:

185. ~~Le Monde, <https://www.lemonde.fr/en/international/article/2022/05/10/spain-fires-head-of-intelligence-services-over-pegasus-ph>~~

185a. ~~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.

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

187. 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.

187a. <https://www.theguardian.com/world/2020/jul/16/two-catalan-politicians-to-take-legal-action-targeting-spyware>

188. 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.

188a. Citizen Lab, *Correcting a case, CatalanGate report* <https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/> 22 December 2022

189. *El Nacional*, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

Covered:

Fall: AM 691 (Greens), AM 692 (Rapporteur)

100 a (new). The Spanish government has given limited information so far on their role in this targeting, invoking the need for confidentiality in relation to national security and legal obligations. However, on the basis of a series of indicators, some of which had been admitted during the aforementioned Official Secrets Committee, it is assumed that the surveillance of the Catalan targets was conducted by the Spanish authorities.

Footnotes:

1a. 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

Paragraph 100b (new)

Covered: AM 693 (Rapporteur), AM 694 (Greens)

Fall: AM 696 (Cañas)

100 b (new). A close analysis of the surveillance shows a clear pattern. Most of the "CatalanGate" interceptions coincide with, and relate to moments of political relevance, such as the admissibility of the disconnection laws by the Catalan Parliament and the court cases against Catalan separatists, public rallies organised by Tsunami Democràtic, and communication with Catalan separatists living outside Spain^{1a}. 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 in what way the targets would have an immediate impact on, or constitute an imminent threat to national security or the integrity of the state, and no information was provided on this^{1b} (AM 693, AM 694). 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 the spyware surveillance^{1c}.

Footnotes:

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

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

1c. Mission to Spain.

COMP 94 (Paragraph 101 to Paragraph 101 a (new))

Covered: 697 (Cañas), 698 (S&D), AM 699 (EPP)

Fall: AM 700 (Greens), AM 701 (Rapporteur)

Purchase of Spyware

101. The *Spanish authorities have acknowledged in the past the purchase of tools for the interception of telecommunications, like the Systems for the Lawful Interception of Telecommunications* ~~various spyware products like SITEL (SITEL)~~ in 2001 and the *contracting of spyware services from* ~~of~~ Hacking Team in 2010 by the Ministry of the Interior, the Spanish National Intelligence Centre (CNI) and *the Spanish National police (AM 699), in the context of the implementation of the Integrated Telecommunications Interception System, providing the operation units of the State Security and Corps (FCSE) with the means for the interception and recording of electronic communications authorised by a court order^{1a}* ~~has been widely publicised¹⁹⁰~~ (AM 698). *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 Finfisher¹⁹¹. In 2020, the Spanish newspaper *El Pais* reported that Spain has done business with NSO Group and that the CNI routinely uses Pegasus¹⁹². The Spanish government allegedly purchased the spyware in the first half of the 2010s for an estimated amount of €6 million^{193 194}. *The purchase of SITEL was confirmed by former Vice-President de la Vega in 2009^{194a}, while the contracting of Hacking Team's services was acknowledged by the CNI in a comment made to the newspaper El Confidencial in 2015^{194b} (AM 699).* In addition, a former employee of NSO has further confirmed that Spain has an account with the company^{194c} despite the Spanish authorities declining to comment or confirm¹⁹⁵.

Footnotes:

1a. 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

~~190 Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 4–5.~~

191. 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.

¹⁹² 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.

193. Politico, <https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/>, 20 April 2022.

194. *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.

194a. Newtral, <https://www.newtral.es/sitel-programa-espia-guardia-civil-policia-espana/20220509/>, 9 May 2022

194b. *El Confidencial*, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/, 6 July 2015

194c. *The New Yorker*, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022

195. *The New Yorker*, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

Covered: AM 702 (Rapporteur)

Fall:

101 a (new). According to Google's Threat Analysis Group (TAG), spyware company Variston IT as based in Barcelona, is allegedly linked to a framework that exploits n-day vulnerabilities in Microsoft Defender, Chrome and Firefox, installing spyware on targeted devices. The vulnerabilities were fixed in 2021 and early 2022^{1a}. According to its website, Variston offers 'tailor made Information Security Solutions'^{1b} (AM 702).

Footnotes:

1a. Threat Analysis Group. New details on commercial spyware vendor Variston.; Techcrunch. Spyware vendor Variston exploited Chrome, Firefox and Windows zero-days, says Google.

1b. <https://variston.net/>

COMP 95 (Paragraph 102 to Paragraph 102 d (new))

Covered: AM 703 (Cañas), AM 704 (S&D),

Fall: AM 705 (ID), AM 706 (EPP)

Legal Framework

102. The right to privacy is protected under Article 18 of the Spanish Constitution of 1978, including the right to "secrecy ~~in~~ **of communication, especially of** 'postal, telegraphic and telephone communication'¹⁹⁶ **which is guaranteed (AM 704)**. The use of spyware such as Pegasus and Candiru ~~is would be~~ a violation of Article 18 ~~however, there is an exception to this right in the case of a court granting authorisation¹⁹⁷ if no judicial authorisation has been granted, but this possibility is provided for under Spanish law^{196a}~~ (AM 703). The constitution also provides further exceptions to those rights in Part I Section 55 by stating that some ~~freedoms~~ **rights** are eligible to be suspended with 'participation of the courts and proper parliamentary control' **when the declaration of the state of emergency or siege is agreed under the terms provided in the Constitution (AM 704)**, in the case of individuals under investigation for activities relating to armed groups or terrorist organisations¹⁹⁸. **Furthermore, Article 55 includes democratic safeguards to ensure that 'unjustified use or misuse' of those powers will give rise to criminal liability (AM 703).**

Footnotes:

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

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

196a. Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, Section 18.

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

Covered: AM 709 (S&D)

Fall:

102 a (new). For activities that may affect the inviolability of the home and the secrecy of communications, article 18 of the Spanish Constitution requires judicial authorization, and article 8 of the European Convention for the Protection of Human Rights (ECHR) and

Fundamental Freedoms requires that this interference is provided for in 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 (AM 709).

Covered: AM 707 (Greens), AM 708 (Rapporteur), AM 710 (S&D), AM 713 (S&D)

Fall:

102 b (new). Further detail on the exemptions to the Article 18 right to privacy is outlined in the Criminal Procedure Act^{1a 1b}. Article 588 of the Act, specifically limiting the use of investigative measures to the investigation of those facts, which, due to their particular seriousness, justify the limitation of fundamental rights. Nevertheless, the cases contemplated 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 alarm, exception and siege"; and c) Provision of Organic Law 2/1989, of 13 April, on Military Procedure, in which the regulation of the Law of Criminal Procedure is supplementary applicable. Article 588 of the Act requires authorisation to be provided by a judge for the interception of telephone and telematic communications when the purpose of the investigation is 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 (AM 713). Authorisations are subject to four specific principles. Firstly, speciality (that the surveillance is related to a specific crime). Secondly, adequacy (outlining duration, objective and the subjective scope). Thirdly, proportionality (strength of existing evidence, severity of the case and result sought), and finally the exceptional nature and necessity (there are no other measures available and without it, the investigation will be interfered with)^{1c}. (AM 707, AM 708, AM 710, AM 713). Article 588 septies (a,b and c) specifically sets the conditions on 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 pursues the investigation of certain criminal offences. To that end, the measure shall have a strict duration of one month, extendable for equal periods up to a maximum of three months (AM 707).

Footnotes:

1a. Criminal Procedure Act 2016, <https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedura%20Act%202016.pdf>

1b. 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>

1c. Criminal Procedure Act 2016, <https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedura%20Act%202016.pdf>.

Covered: AM 711 (Greens), AM 712 (Rapporteur)

Fall:

102 c (new). *Article 197 of the Criminal Code sets out a one to four-year prison sentence and penalty of 12 to 24 months for persons who seize or intercept i.a. electronic mail and telecommunications without correct permission^{1a}. Additionally, Article 264 of the Code of Criminal Procedure further regulates this area in relation to the criminal act of erasing or deleting of data, and allows for gaining access to the data in situations where the required authorisation has been granted by a competent authority^{1b} (AM 711, AM 712).*

Footnotes:

1a. Criminal Code 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, at Article 197.

1b. Criminal Procedure Act, 2016 <https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedu re%20Act%202016.pdf> at Article 264.

Covered: AM 714 (S&D)

Fall:

102 d (new). *Regarding the judicial control, the following requirements must be complied with: a) That the judicial police inform the examining magistrate of the development and results of the measure; b) That the judge establishes in the enabling judicial decision the frequency and form in which the judicial police must inform him/her of the development of the measure; c) That the Judicial Police should make available to the judge, within the established deadlines, two different digital supports, one with the transcription of the passages considered to be of interest and the other with the complete recordings made; d) That the recordings indicate the origin and destination of each of the communications; e) That the Judicial Police ensure, by means of an advanced electronic sealing or signature system or a sufficiently reliable warning system, 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) That the judicial police report the results of the measure when the measure is terminated (AM 714).*

COMP 96 (Paragraph 103 to Paragraph 103 a (new))

Covered: AM 715 (Left), AM 716 (Cañas), AM 717 (S&D)

Fall: AM 718 (Greens), AM 719 (Rapporteur)

103. 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 (AM 715) and which acts under the supervision and control of the executive, legislative and judicial powers and is attached to (AM 717) – is under the control of the Ministry of Defence^{1a}. 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-intelligence¹⁹⁹. The second body is the domestic intelligence agency, the Intelligence Centre for Counter-Terrorism and Organised Crime (CITCO). The third and final body is the Spanish Armed Forces Intelligence Centre (CIFAS). The CIFAS is also under the direct supervision of the Ministry of Defence^{200 201}. *The CNI was established under Law No 11/2002 of 6 May 2002, pursuant to which it is authorised to conduct 'security investigations'^{201a} (AM 716). The country's police and**

law enforcement agency, known as the "Guardia Civil", is of a "military nature", and also accountable to the Ministry of Defense^{201b} (AM 715).

Footnotes :

1a. National Intelligence Centre (CNI), <https://www.cni.es/>

199. <https://www.cni.es/en/intelligence>

200. https://emad.defensa.gob.es/en/?_locale=en

201. Geneva Centre for Security Sector Governance report 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf at pg. 40.

201a. 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.

201b. <https://www.guardiacivil.es/es/institucional/Conocenos/index.html>

Covered: 720 (Left), 732 (Greens), 733 (Rapporteur)

Fall:

103 a (new). The Official Secrets Law, which dates back to 1968 ensures that when a document is classified in Spain, does not outline a declassification time period beyond which an official secret would expire^{1a}. 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 will remain secret. This law is currently under revision by the Spanish government, and though no deadline has been set for its adoption (AM 720, AM 732, AM 733), the preliminary draft law on classified information was approved on 1 August 2022. It establishes that classified information will have to be published within a period between four and 50 years, although this may be extendable.

Footnotes:

1a. 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.

COMP 97 (Paragraph 104 to Paragraph 104 a (new))

Ex-ante Scrutiny

Covered: AM 721 (S&D), 722 (Cañas), 724 (EPP)

Fall: 723 (ECR), 725 (ID)

104. 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 ~~a body that has been embroiled in a number of scandals relating to surveillance in the past²⁰²~~. The CNI was established under Law 11/2002 May 6 and it ~~authorises~~ **grants** the CNI **powers** to conduct ‘security investigations’²⁰³ **on persons or entities^{203a}**. However, there is little clarification on the means or limitations of such

activities²⁰⁴ *as the CNI activities, as well as 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, constitute classified information, with the degree of secrecy^{204a} (AM 721).* Law 11/2002 also established parliamentary, executive and legislative oversight control over the CNI²⁰⁵ Parliamentary oversight is to be carried out by *the Committee on the use and control of credits allocated to secret funds (the so-called Official Secrets Committee) (AM 721)* of the Spanish Congress, which was established in 1995²⁰⁶. *Because of a delayed establishment of the committee during the 14th term of the Spanish Parliament, constituted in December 2019, the Official Secrets Committee did not submit the annual report on the activities of the CNI, as it has the prerogative by law. Until April 2023, no annual report has been submitted during this parliamentary term.* The **Government** Delegated Committee for Intelligence Affairs ~~is in executive control of the body, and~~ co-ordinates the intelligence activities of ~~the~~ *all Spanish CNI²⁰⁷ intelligence and information services^{206a}*. Lastly, the Defence Committee of the Congress of Deputies conducts legislative oversight over the CNI²⁰⁸. The annual Intelligence Directive ~~dietates~~ *sets* the intelligence priorities for the CNI ~~for the year²⁰⁹~~.

Footnotes:

202. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spywareoperation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 2
203. 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.
- 203a. 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.
204. OMCT, <https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain>, 4 May 2022.
- 204a. Law 11/2002, of May 6, Regulating the National Intelligence Centre, at Article 5.1.
205. 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.
206. Law 11/1995 May 11, <https://www.boe.es/eli/es/l/1995/05/11/11/con>.
207. 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.
- 206a. 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.
208. 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.
209. ~~On Balance: Intelligence Democratization in Post-Franco Spain, <https://www.tandfonline.com/doi/full/10.1080/08850607.2018.1466588?scroll-top&needAccess=true>, International Journal of Intelligence and Counter intelligence [2018] Vol 31 issue 4, 769-804 at pg. 776.~~

Covered: 726 (Greens), 727 (Rapporteur), 728 (EPP), 729 (S&D), 730 (S&D)

Fall:

104 a (new). *Judicial control over the actions of the CNI is provided for in Organic Law 2/2002 May 6^{1a 1b}, which is complementary to Law 11/2002 of 7 May, regulating the National Intelligence Centre. In particular, this regulation requires that when the CNI seeks to conduct surveillance, the CNI Secretary of State Director of CNI has the obligation to request authorization 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^{1c}, provided that such actions are necessary for the fulfillment of the functions assigned to the centre. In addition, the law*

stipulates that surveillance operations cannot last more than three months, and any extension of said term must be properly justified. However, these provisions were brought in to 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 the reform of the legal framework of the CNI, but no proposals have been submitted yet (AM 726, AM 727, AM 728, AM 729, AM 730).

Footnotes:

- 1a. OMCT, <https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain>, 4 May 2022.
- 1b. 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>.
- 1c. OMCT, <https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain>, 4 May 2022

COMP 98 (Paragraph 105 to Paragraph 105 a (new))

Covers: 734 (Left), 735 (S&D), 737 (EPP), 738 (Cañas),

Falls: 736 (ECR), 739 (ID)

Ex-post Scrutiny

105. The laws establishing the CNI also established the Defence Committee of the Congress of Deputies and it **which** is responsible for allocating the ~~confidential~~**secret** funds for the CNI and producing an annual report on the CNI. ~~However, the Spanish Constitution does not stipulate that access will be granted to documents or information relating to the work of the intelligence services and the requirement is also notably absent in the legal framework of the law on transparency. Therefore, much of the work of the CNI is kept secret and lacks transparency²¹⁰.~~ *The amounts assigned to secret funds are set in the Spanish general budget law for each financial year^{1a}. All the bodies that are tasked with oversight of the CNI, such as the Defence Committee or the Official Secrets Committee or the Ombudsman, have access to the information necessary to assess whether operations were pursued lawfully and correctly (AM 737). The Government determines and approves annually the objectives of the CNI through the Intelligence Directive, which is secret^{1b 1c}. The Director of the CNI has exclusive competencies on determining the purpose and destination of the funds assigned, and periodically has to report on their use to the Head of the Government. The Committee on the use and control of credits allocated to secret funds is informed about the intelligence objectives, has the prerogative to submit an annual report on the activities of the intelligence services^{1d}, and has access to the annual report produced on a yearly basis by the Director of the CNI on the assessment of activities, status, and degree of fulfilment of the objectives (AM 735). However, the Spanish Law does not stipulate that public access will be granted to documents or information relating to the work of the intelligence services and the requirement is also notably absent in the legal framework of the law on transparency^{1e}. (AM 738). As a consequence of the secrecy, it cannot be determined with certitude that the Spanish government has concluded any contracts with NSO Group and whether it has acquired and used Pegasus. The persons targeted*

do not know the reasons, scope and consequences of the interception of their communications^{lf} (AM 734).

Footnotes:

210. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spywareoperation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 2.

1a. 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>

1b. Law 11/2002, of May 6, regulating the Intelligence Nacional Centre (CNI), at Article 3.

1c. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022, p. 2.

1d. Law 11/1995, of May 11, regulating the use and control of credits allocated to secret funds, at Article 7.4.

1e. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 2.

1f. Amnesty International - 10 medidas que garanticen la no repetición de violaciones de Derechos Humanos

Covers: 740 (Greens), 741 (Rapporteur), 742 (S&D), 754 (S&D), 755 (Cañas), AM 895 (EPP)

Fall:

105 a (new). As result of the revelation that the CNI has used Pegasus and Candiru, the Spanish Ombudsman announced an ex officio investigation^{1a}. The Spanish Ombudsman recognised in its official statement of 18 May 2022 that the Council of Ministers granted full access to classified documents to the Ombudsman to their examination, not making use of its prerogative provided for in Article 22 of Organic Law 3/1981 on the Ombudsman (AM 754). However, this investigation was only concerning the 18 persons that the Spanish authorities have confirmed they targeted with court authorisation^{1b 1c}. The investigation concluded that the interception had been carried out within the law, by establishing that they had been approved by a court and the authorisation was accompanied by the required motivation^{1d 1e} (AM 742, AM 755). However, the Ombudsman does not have the competence to assess the proportionality, which can only be established by a judge^{1f}. He also did not contact or interview any of the targeted persons, or their lawyers. The Ombudsman recommended a review of the existing legal provisions and make reforms where necessary to reflect the modernisation of surveillance systems^{1g}. On foot of this, the Spanish government announced in May 2022 that there would be a review conducted on the Official Secrets Act of 1968, and the Organic Law Regulating Prior Judicial Control of the CNI (Law 2/2002)^{1h1i} (AM 740, AM 741, AM 895), but no deadline has been set for adoption of this review.

Footnotes:

1a. <https://www.reuters.com/article/us-spain-politics-catalonia-spying-idCAKCN2MG0A6>, 24 April 2022

1b. The Guardian, <https://www.theguardian.com/world/2022/may/05/catalans-demand-answers-after-spanish-spy-chief-confirms-phone-hacking>, 5 May 2022.

1c. <https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/>

1d. La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26 May 2022.

1e. La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26 May 2022.

1f. Information from Mission to Spain

1g. <https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha->

realizado-conforme-la-constitucion-la-ley-los-casos-examinados/

1h. El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

li. La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26 May 2022.

COMP 99 (Paragraph 106 to Paragraph 106 b (new))

Covered: 743 (Greens), 744 (Rapporteur), 746 (Cañas), 748 (Left), 749 (EPP)

Fall: 747 (ID), 750 (ECR)

106. The Official Secrets Committee *on the use and control of the credits allocated to secret funds* is required to submit an annual report on the activities of the intelligence services ~~;~~ however *However* when it was convened *on May 5th 2022*, as a result ~~in view~~ of the surveillance by the CNI, it was the first meeting of the body in more than ~~two~~ *three* years, *as a result of the disruption of parliamentary activity caused by the Covid pandemic (AM 749)*. Head of the CNI Paz Esteban appeared before the Committee, *admitted to the surveillance of 18 leaders of the separatist movement and on 5 May 2022 to present presented* the court authorisations for *those 18 cases* the 18 victims that the authorities have taken responsibility for targeting^{211 211a}. *However, in accordance with article 5.5 of law 11/2002, the* The hearing was not public *conducted in camera* and those present were not allowed to enter with any electronic ~~on them whatsoever~~²¹² *devices*^{211b}. *No official communication was made, with the exception of the number of cases. According to the spokespersons present at the hearing, it was almost solely focused on the Catalan targets, and not on Pedro Sanchez and Margarita Robles and the alleged 3GB of data that was taken from their devices by mercenary spyware*^{211c}. *Robles has repeatedly insisted that the targeting of the 18 Catalans-targets was valid (AM 743, AM 744, AM 746, AM 748).*

Footnotes:

211. El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

211a. 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

212. El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

211b. El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

211c. El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

Covered: 752 (Greens), 753 (Rapporteur)

Fall:

106 a (new). Sanchez has also spoken on the issue in the Spanish Congress, where he once again reiterated that everything has been done within the law, and that national security is subject to the control of parliament and other government bodies^{1a}. The idea that the use of Pegasus was entirely legal, was also claimed by former NSO Group

CEO Shalev Hulio, who told the New Yorker that the use of Pegasus by Spain was legitimate given Spain's strong respect for the rule of law and requirement for Supreme Court authorisation^{1b} (AM 752, AM 753).

Footnotes:

1a. *La Moncloa*, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx , 26 May 2022.

1b. *The New Yorker*, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens> , 18 April 2022.

Covered: 745 (Puigdemont)

106 b (new). On 3 May 2022 the Spanish Congress voted down a proposal to establish a committee of investigation 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 (AM 745)

COMP 100 (Paragraph 107)

Covered: 761 (rapporteur), 762 (Puigdemont), 763-768 (Cañas)

Falls: 756 (Cañas), 757 (EPP), AM 758 (S&D), (759 (The Left), 760 (ECR)

Public Scrutiny

107. There has been a significant amount of public scrutiny on the ‘~~CatalanGate~~’ ~~scandal~~ case ***of the use of spyware against members of the Spanish government and Catalan advocates of independence***, since it came to light in April 2022. The Spanish media and media outlets around the world have worked extensively in conjunction with civil society organisations to scrutinise the surveillance system in Spain and advocate for the fundamental rights of the ***persons targeted*** ~~victims~~. Inversely, some Spanish politicians have tried to discredit Citizen Lab, suggesting their methods are unsound or that they are politically motivated. ~~A collaborator of Citizen Lab, himself of Catalan origin, was among the targets, along with his parents, who are not politically active at all²¹³.~~

Footnotes:

213 *Dit Kan Geen Toeval Zijn*, *De Volkskrant* podcast series by Huib Modderkolk and Simone Eleveld, 2022.

COMP 101 (Paragraph 108)

Covered: 769 (S&D)

Fall: 770 (Cañas), 771 (Cañas),

Redress

108. A legal case regarding the *spyware* surveillance of Prime Minister **Pedro** Sánchez and Minister for Defence **Margarita** Robles was filed in Madrid in the Audiencia Nacional, the Spanish National Court (SNC), by the state solicitors' office²¹⁴ **in Madrid's Spanish National Court (SNC), the Audiencia Nacional. The alleged facts fall within the jurisdiction of the SNC, as established in Article 65.1a of the Organic Law 6/1985 of the judiciary, as they affect high ranking national bodies, such as the President of the Government and the Minister of Defence (AM 769).** Judge Jose Luis Calama, head of the Central Court of Instruction number 4, is responsible for this on-going case²¹⁵. On 13 October 2022, Judge Calama delivered a questionnaire to both Robles and Grande-Marlaska, which included a request, to be confirmed by legal sources, as to how the Pegasus infections were identified. The Prosecutors Office and the Office of the State Attorney also sent questions to the Ministers²¹⁶.

Footnotes:

214. El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.
215. El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.
216. El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

COMP 102 (Paragraph 109)

Covered: 774 (Greens), 775 (S&D), 776 (ID), 777 (EPP), 782-783 (NI)

Fall: 772 (Cañas), 773 (ECR), ,

109. ~~In contrast to the fast paced nature of the case taken by Sanchez et al. in Madrid, the cases that have been filed in Barcelona by Catalanian victims of spyware are moving at a slow pace²¹⁷⁻²¹⁸.~~ **Legal complaints on spyware surveillance have been filed in Investigative Court in Barcelona by individuals with direct or indirect ties to the pro-Catalan independence movement, and investigations are ongoing, but moving at a slow pace (AM 775).** The first case **complaint** in Investigative Court number 32 in Barcelona was filed by two Pegasus victims in 2020 **by** former President of the Catalan Parliament and current Minister of Business and Work, Roger Torrent, and former Minister of Foreign Action, Institutional Relations and Transparency of Catalonia and current ERC President in Barcelona City Council, Ernest Maragall^{219 219a}, **and 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 is ~~a victim targeted with~~ of Pegasus himself. Van Den Eynde has criticised the courts consistently delaying proceedings and virtually 'paralysing' the case²²⁰. Òmnium Cultural, **Catalan National Assembly (ANC)** and the Popular Unity Candidacy party (CUP) have also filed ~~a case~~ **several criminal complaints** in the same court in Barcelona, **but no investigation has yet been opened.** ~~Lawyer Benet Salellas, who is involved in both cases, is asserting that the Spanish government is behind the targeting²²¹.~~ **Investigative Court number 32 in Barcelona rejected to accumulate the lawsuits and now they are dealt with by different courts and judges (AM 783). 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 admitted, nor has it been agreed to carry out any investigative diligence and nothing is being investigated for any of those cases (AM 774). Most of the cases have been shelved by the judges until more evidence is gathered, since the key piece of evidence, i.e. the allegedly infected mobile phones, were not available to the plaintiffs anymore^{220a} (AM 777). Judges may decide whether or not to accept the reports by Citizen Lab as expert evidence in the court case, which makes it difficult for the targeted persons to prove their case^{220b}.

Footnotes

217. *El Diario*, https://www.eldiario.es/catalunya/juez-barcelona-no-ve-base-imputar-empresa-pegasus-espionaje_1_9068271.html, 9 June 2022.

218. *El Diario*, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30 May 2022.

219. *El Nacional*, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

219a. *El Diario*, https://www.eldiario.es/catalunya/juez-archiva-investigacion-espionaje-pegasus-torrent-maragall_1_9030414.html, 30 May 2020

220. *El Diario*, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30 May 2022.

221. *El Nacional*, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-nationalaudience_750840_102.html, 2 May 2022.

220a. *El País*, <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.

220b. *Mission to Spain*

COMP 103 (Paragraph 110)

Covered:

Fall: 778 (S&D), 779 (ECR), 780 (ID), 781 (Canas)

110. As the SNC has jurisdiction over cases concerning the most serious crimes in all territories, it is possible that the public prosecutor could request all Pegasus cases to be unified²²². In other words, the cases of the ~~vietims~~ **targets** from the Spanish government and the ‘CatalanGate’ ~~vietims~~ **targets** would all be heard in the SNC in Madrid. The lawyers representing the Catalan ~~vietims~~ **targets** assert that there is no link between the cases unless the perpetrator is proved to be the same in all instances of surveillance²²³.

Footnotes:

222. *El Nacional*, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

223. *El Nacional*, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

COMP 104 (Paragraph 111)

Covered: 788 (Greens)

Fall: 784 (Cañas), 785 (EPP), 786 (S&D), 787 (ECR), 789-790 (NI), 791 (Cañas)

111. There are a number of other pending legal cases linked to the 65 Catalan **targets** ~~vietims~~. One such case was filed by lawyer and Pegasus ~~vietim~~ **target** Gonzalo Boye on behalf of

at least 19 ~~victims~~ **targets** against NSO, its three founders Niv Karmi, Shalev Hulio and Omri Lavie, Q Cyber Technologies, and OSY, a subsidiary company based in Luxembourg^{224 225}. *Former President of Catalonia Quim Torra and former Vice-President of the Catalan Parliament Josep Costa, have filed a complaint with 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 Spanish National Court. No investigation has taken place in the meantime (AM 788).* Legal action is also underway in a number of other EU Member States as a result of the surveillance carried out on those Catalan separatists in exile, including France, Belgium, Switzerland, Germany, and Luxembourg²²⁶.

Footnotes:

224. *El Nacional*, https://www.elnacional.cat/en/politics/boya-catalangate-legal-offensive-pegasus_751530_102.html, 3 May 2022.

225. *Catalan News*, <https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab>, 19 April 2022.

226. *Catalan News*, <https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab>, 19 April 2022.

COMP 105 (Paragraph 112)

Covered: AM 792 (S&D), AM 793 (S&D), 796 (S&D), 798 (Greens)

Fall: 794 (Cañas), 795 (ECR), 797 (NI), 799 (EPP), AM 800 (Greens), AM 801 (ECR),

Political Targets (AM 792)

112. The targeting *with spyware* of *members of the Catalan pro-independence movement and family and staff relating to these people* ~~citizens with spyware reportedly 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 had been targeted with spyware between 2017 and 2020: 63 with Pegasus, four with Candiru and at least two people with both^{1a}. At least 51 individuals were successfully infected^{1b} 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 (AM 796).* ~~and has been carried out on a large scale since 2017²²⁷. After initial media coverage in 2020, the full scandal broke across Europe in April 2022 with the publication of the University of Toronto CitizenLab report. 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 investigated owing to various factors that occurred, including a number of targets who disposed of the phone in question²²⁸.~~

Footnotes:

1a. *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.

1b. 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.

227 <https://catalonia.citizenlab.ca/#targeting-puigdemont>

228 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.

COMP 106 (Paragraph 113)

Covered: 793 (S&D)

Fall: AM 802 (S&D), 803 (EPP), 804 (Cañas), 805 (NI)

113. 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 2021²²⁹. There is little information available so far on details of this hacking, as they were announced by the government and were not the result of an investigation of CitizenLab or any other such research service or 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^{230 230a}. Grande-Marlaska was infected on his personal device²³¹. Minister for Agriculture Luis Planas, who formerly served as a diplomat in Morocco, was also targeted with spyware but there was no successful infection. It has been reported that the Moroccan government could potentially be responsible for this targeting, however that information has not been confirmed²³².

Footnotes:

229. *El Nacional*, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

230. *The Economist*, <https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099>, 7 May 2022.

230a. *ElEsanol*, https://www.elespanol.com/espana/20220707/interior-corrige-pegasus-marlaska-infectado-no-personal/685681761_0.html 7 July 2022

231. *La Razon*,

232. *The Economist*, <https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099>, 7 May 2022.

COMP 107 (Paragraph 114)

Covered: 808 (rapporteur), 809 (Greens), 811 (The Left), 812 (EPP), 813 (NI)

Fall: 806 (S&D), 807 (ECR), 810 (Cañas), 814 (EPP), 815 (The Left), 816 (The Left)

114. ~~In total 65 Catalans were confirmed to have been targeted with mercenary spyware, 63 with Pegasus, four with Candiru and at least two people were targeted by both²³³. At least 51 individuals were successfully infected²³⁴. 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^{234a}. It remains unclear whether or not the other individuals were targeted by the CNI a Court order or whether or not another authority had received Court orders to legally target them. The Spanish government have refused to comment as to whether or not they were responsible for the surveillance~~

any of the other victims outside of the 18 they admit to having targeted²³⁵. *Despite the court warrants for the use of spyware on 18 persons, they were not subsequently the majority of those 18 persons were never charged with any crime relating to the warrant authorising the use of spyware. Among the targets for which 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^{235a} (AM 808, AM 809). Subject to the requirements of secrecy and confidentiality contained in the law, Minister for Defence Robles has relied heavily on referred to the Official Secrets Act rather than for not expanding on what were the reasons for the surveillance of those specific targets²³⁶. Most of the All 65 Catalan targets have at some point in time been in contact with the members of the pro-Catalan independence movement separatists living outside Spain (AM 813). Some of the persons targeted were outside Spain at the moment of the infection, as in Belgium, Switzerland, Germany and France. Such digital surveillance would be illegal in Germany, unless expressly permitted by the federal authorities (AM 811).*

Footnotes:

233. 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.

234. El Nacional, <https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge-752448-102.html>, 5 May 2022.

234a. El Nacional, <https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge-752448-102.html>, 5 May 2022.

235. El Nacional, <https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge-752448-102.html>, 5 May 2022.

235a. El Nacional, <https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge-752448-102.html>, 5 May 2022.

236. El Nacional, <https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge-752448-102.html>, 5 May 2022.

COMP 108 (Paragraph 115 to Paragraph 115 d (new))

Covered: 817 (S&D), 818 (Cañas)

Fall:

Members of the European Parliament (AM 817, AM 818)

Covered: 820 (EPP), 821 (NI), 822 (Greens), 823 (Cañas), 824 (rapporteur)

Fall: 819 (S&D), 825 (ECR), 828 (Cañas)

115. 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 CitizenLab refer to as relational targeting²³⁷: Diana Riba i Giner, Antoni Comín i Oliveres, Jordi Solé, Carles Puigdemont, and Clara Ponsati. *The mobile phone of a former accredited assistant of Mrs 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 due to an error in labelling of initials.*

Footnotes:

237. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg.6.

Covered: 826 (Greens), 827 (Rapporteur)

Fall:

115 a (new). *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 the 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^{1a}. Riba i Giner outlined at a hearing of the Pegasus Committee of Inquiry in the European Parliament that at that time, the majority of her phone calls were regarding 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^{1b} (AM 826, AM 827).*

Footnotes:

1a. 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.

1b. 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.

Covered: 829 (Greens), 830 (Rapporteur)

Fall:

115 b (new). *Jordi Solé MEP, also of ERC was originally reported to have been hacked on both the 11th and 27th of June 2020 according to the research of CitizenLab.^{1a} However, five further attacks during the same period were later discovered^{1b}. 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^{1c}. Similar 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^{1d} and only one month before Solé was appointed to take over that seat in July 2020. Additionally, there were on-going discussions at that time on party strategy and international litigation regarding their imprisoned and exiled colleagues during the time of the infections^{1e} (AM 829, AM 830).*

Footnote:

1a. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 7

1b. Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Mr. Jordi Solé MEP, Strasbourg 6 October 2022.

1c. The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

1d. Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Mr. Jordi Solé MEP, Strasbourg 6 October 2022.

1e. Politico, <https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/>, 9 January 2020

Covered: 832 (Greens), 833 (Rapporteur)

Fall: AM 831 (Rapporteur)

115 c (new). Carles Puigdemont MEP for JUNTS and former President of Catalonia was targeted through his spouse Marcela Topor, members of staff and a number of his associates^{1a}. In total, CitizenLab 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^{1b} (AM 832, AM 833).

Footnotes:

1a. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 7.

1b. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 8.

Covered: AM 834 (Greens), AM 835 (Rapporteur)

Fall:

115 d (new). Clara Ponsatí, MEP for JUNTS, former Minister of Education of Catalonia, was victim of relational targeting. Pol Cruz, a staff member at the European Parliament, was confirmed to have been infected on July 7th 2020^{1a} (AM 834, AM 835).

Footnotes:

1a. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 7.

Covered: AM 836 (S&D), AM 837 (Cañas)

Fall:

COMP 108 (Paragraph 116)

Covered:

Fall: 838 (S&D), 839 (ECR), 840 (Cañas), 841 (NI), 842 (EPP), 843, 844 (NI)

Catalonian Politicians (AM 836, 837)

~~116. Former President of the Catalanian Parliament and current Minister of Business and Work Roger Torrent was among the first persons to come forward as a victim of the 2019 WhatsApp Pegasus infections²³⁸. Shortly after, leader of the pro-independence Republican Left of Catalonia Party, Ernest Maragall and Anna Gabriel who was previously a regional Member of Parliament for the Popular Unity Candidacy party also~~

came forward as victims of Pegasus²³⁹. All of the Presidents of Catalonia since 2010 have been targeted with spyware either during or after their term in office²⁴⁰. 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 CitizenLab. It is highly significant that both Gabriel and Rovira were living in Switzerland at the time of their surveillance following the fall out after the 2017 referendum.

Footnotes:

238. *The Guardian*, <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>, 13 July 2020.

239. *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.

240. Artur Mas (after leaving office), Carles Puigdemont (relational targeting), Joaquim Torra (while in office), Pere Aragonés (infected while serving as Torra's Vice President). <https://catalonia.citizenlab.ca/>

COMP 110 (Paragraph 117 to Paragraph 117 d (new))

Covered: 845 (Cañas), 846 (ECR), 847 (S&D), 848 (S&D),

Fall: 862 (NI)

~~Civil Society Organisations~~ **Civilian targets, including journalists, lawyers and civil society representatives (AM 845, 846, 847, 848)**

Covered: 852 (EPP), 853 (Greens)

Fall: 849 (Cañas), 850 (S&D), 851 (ECR)

117. Jordi Domingo was one of the first Catalan activists that was reported to be targeted in 2020. Though a supporter of Catalan independence **and member of the Catalan National Assembly (ANC) (AM 853)**, 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 **the a potential constitution of for an independent (AM 852) Catalonia**²⁴¹.

Footnotes:

241. *The Guardian*, <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>, 13 July 2020.

Paragraph 117a (new)

Covered: 854 (Greens), 855 (NI), 861 (The Left)

Fall:

117 a (new). The Catalan National Assembly (ANC), a Catalan civil society organization supporting Catalan independence was one of the first organizations targeted prior to the Catalan referendum, and has since been subject to extensive targeting^{1a}. The six targets of the ANC include two of her former presidents, Jordi Sanchez (2015-2017)

and Elisenda Paluzie (2018-2022), whose spyware surveillance was granted by court order, as it was that of expert in digital voting and decentralisation, Jordi Baylina, two members of its National Board (Arià Bayè and Sònia Urpí), one member of a local branch (Jordi Domingo) (AM 854, AM 855, AM 861).

Footnotes:

1a. CitizenLab's CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>

Covered: 856 (The Left)

Fall: 859 (Rapporteur), 863 (Greens)

117 b (new). The people close to Jordi Cuixart, president of Òmnium Cultural (until February 2022) were infected as he was imprisoned during the time, Marcel Mauri, serving as a Vice President of the NGO, whose spyware surveillance was granted by court order.

Covered: 857 (Rapporteur), 858 (Greens)

Fall:

117 c (new). CitizenLab discovered an active Candiru infection on the laptop of Joan Matamala, a business man and activist with close ties to pro-independent Catalan politicians in February 2021^{1a}. 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 CitizenLab to better understand its patterns. Subsequently, 16 other infections on Matamala's device were discovered^{1b}. Microsoft subsequently patched the vulnerabilities through updates but it is impossible to know the number of Candiru infections that have gone unnoticed^{1c} (AM 857, AM 858).

Footnotes:

1a. The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

1b. The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

1c. The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

Covered: 860 (NI), 864 (NI)

Fall:

117 d (new). 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^{1a}. Vives and Escrich's spyware surveillance was authorised by a court order. (AM 860, AM 864)

Footnotes:

1a. <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#finding-catalans-targeted-with-candiru>

COMP 111 (Paragraph 118)

Covered: AM 869 (Cañas), AM 870 (ECR), AM 871 (S&D)

Fall:

~~Lawyers~~ (AM 869, 870, 871)

Covered: 874 (Cañas), 875 (EPP)

Fall: 872 (ECR), 873 (S&D)

118. Gonzalo Boye ~~has represented many high-profile Catalan figures, including~~ **is the lawyer of** former Presidents Puigdemont and Torras²⁴². ~~During the~~ **During the** Over five months between January and May of 2020, ~~he was a victim of Pegasus himself~~²⁴³. Boye was targeted as many as 18 times ~~during that period~~ **(AM 874)** via text messages that appeared as tweets from civil society organisations or prominent news outlets²⁴⁴. CitizenLab confirmed at least one successful infection on 30 October 2020. The infection came just 48 hours after the arrest of one of his client²⁴⁵. **The targeting of Boye has called in to question the legality of attacking the lawyer-client privilege (AM 875).**

Footnotes:

242. <https://catalonia.citizenlab.ca/>

243. <https://catalonia.citizenlab.ca/>

244. <https://catalonia.citizenlab.ca/>

245. <https://catalonia.citizenlab.ca/>

Covered: AM 877 (Greens), AM 878 (Rapporteur)

Fall:

- 118 a (new). 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 for the ECtHR. So far, CitizenLab have only examined Jimenez's latest mobile phone, but they have 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 that he appeared on Catalan television on behalf of Òmnium for the first time (AM 877, AM 878).**

COMP 112 (Paragraph 119)

Covered:

Fall: 880, 881 (identical; S&D, ECR), 882 (Cañas)

119. Andreu van den Eynde i Adroer, was successfully infected with Pegasus on 14 May 2020²⁴⁶. The hacking occurred while he was acting as the lawyer of both Raul Romeva and Oriol Junqueras in their case before the Supreme Court.

Footnotes:

246. Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg.10.

COMP 113 (Paragraph 120 to Paragraph 120 c (new))

Covered: 886 (EPP)

Fall: 885 (Cañas)

120. Similarly, ~~prominent~~ (AM 886) lawyer Jaume Alonso-Cuevillas was also infected while representing key Catalan figures such as Carles Puigdemont. However, CitizenLab were unable to determine the precise date of the successful infection.

Covered: 887 (EPP), 888 (Greens), 876 (S&D), 889 (S&D), 890 (S&D), 891 (EPP), 892 (Greens), AM 893 (Greens), 894 (EPP), 895 (EPP), 896 (Greens)

Fall:

Title (New). Investigations and legal reforms (AM 888, AM 889)

120 a (new). After the allegations contained in the “Catalangate” case came to the light on April 22nd 2022, the Spanish institutions started a process of scrutiny aimed at ensuring that guidelines of surveillance had been applied correctly. These measures involved the summon of Paz Esteban, the director of the CNI to the Official Secrets Committee on may 5th, announced by Minister of the Presidency Felix Bolaños; the session of parliamentary control to the government and the Minister of Defence on the 26th and 27th of April and the independent assessment conducted by the Ombudsman, commenced on April 26th and concluded on May 18th (AM 887, AM 892). The Minister of Defence Margarita Robles, while bound by secrecy per 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^{1a} (AM 894). 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^{1b 1c} (AM 891).

Footnotes:

1a. 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

1b. La Vanguardia, <https://www.lavanguardia.com/politica/20220505/8245084/cni-aporta-autorizaciones-judiciales-parte-espionaje-catalangate.html>, 5 May 2022

1c. El Periodico de Espana, <https://www.epe.es/es/politica/20220505/frente-comun-pp-vox-cs-13614030>, 5 May 2022

120 b (new). *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 judiciary control, and ensure maximum respect for 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 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, upon request of a judge.*

4. *the reform of the 1968 Spanish Law on Official Secrets^{1a 1b}*

5. *the reform of the legal framework of the CNI^{1c}*

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 (AM 876, AM 890)*

Footnotes:

1a. *The reform of the 1968 Spanish Law on Official Secrets*

1b. *El País, El Gobierno inicia la reforma de la ley franquista de secretos oficiales, 5 April 2021*

1c. *La Moncloa, Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías, 26 May 2022*

120 c (new). *Spain's High Court^{1a} opened its own investigation after the government said Pegasus software was 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^{1b 1c}, as well as the Defence and Interior Ministers, whose devices were among those hacked. The Court^{1d} 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 has also lifted the secrecy of the documents related to the case and overturned a ban on investigating wiretapping of mobile phones belonging to Prime Minister Pedro Sánchez and Defence Minister Margarita Robles (AM 893).*

Footnotes:

1a. <https://www.reuters.com/world/spanish-court-calls-ceo-israels-nso-group-testify-case-spying-with-pegasus-2022-06-07>

1b. https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html

1c. <https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations>

1d. <https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations>

Concluding remarks

120 d (new). Spain has an independent justice system with sufficient safeguards. However, following the discovering of the two categories of targets in Spain, there are still some questions, which could be answered by swift and profound reforms and effective implementation. The Spanish government is working on modifications to address shortcomings. Regarding 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^{1a}, the government submitted the legislative amendments of the Official Secrets Law. The government is currently awaiting the opinion of the Council of State.

120 e (new). 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 access to justice, and an investigation should be launched in order to shed light on these cases.

120 f (new). With regard to the 18 cases for which a court order had been issued, the legality has been verified and confirmed by the Ombudsman, but their speciality, adequacy, exceptional nature, proportionality and necessity^{1a} can only be verified by a court.

120 g (new). More generally, judicial proceedings by individuals targeted are not going as quickly as hoped for, in order to provide transparency, and access to meaningful legal remedy. Cooperation by the authorities is crucial here. In order to provide more clarity and contribute with technical expertise, Europol could be invited and support that proper forensic process will be followed.

Foonote:

1a Article 588 a. i., Chapter IV, Criminal Procedure Act

Compromises Other Member States

CA The Netherlands

Paragraph 128 to -129 b (new)

Covered: 908 (EPP), 909 (rapporteur), 910 (Greens), 911 (EPP), 912 (rapporteur), 913 (Greens), 914 (rapporteur), 915 (Greens), 916 (rapporteur),
Falls: 907 (ECR)

The Netherlands

128. The 2017 coalition agreement of the Dutch Government states that the Dutch police *are* ~~is~~ 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* ~~has~~ to ask the provider whether it has provided *spyware* to ~~to EU or UN-sanctioned~~ countries *which have been sanctioned either by the EU or by the UN* and *carry out* ~~performs~~ a check *on whether* if the country where the provider is based has an export control regime *in which* ~~where~~ human rights are assessed in the export licence 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* ~~does use~~ hacking software since 2019, although the authorities do not mention which type²⁴⁹. It would appear that NSO Group and its spyware product Pegasus do not meet the abovementioned standards, in any case not before the tightening of Israel’s export regime in December 2021²⁵⁰. No insight has been given into the expenditure by both police and intelligence services for the purchase and use of the spyware system.

Footnotes:

249 <https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z10593&did=2022D26790>.

250 <https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021>.

128 a (new). *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. (908)*

128 b (new). *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 Netherlands, in the ‘financial holdings’ and ‘engineers and other technical design and advice’ sectors. Both were liquidated after two years in operation^{1a}. (909, 910).*

Footnote:

1a Amnesty International, Operating from the Shadows: Inside NSO Group's Corporate Structure, <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>.

129. 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 spyware²⁵¹. ***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 deadline for signing the contract signatures was approaching***^{251a}. It is not clear whether or not the contract was signed and any spyware was provided to the Dutch Ministry of Defence. (912, 913)

Footnotes:

251 <https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/>.

251a <https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/>.

129 a (new). 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^{1a}. ***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***^{1b}. ***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***^{1c}. (916)

Footnotes:

1a Volkskrant: 'Achterdeur in het nationale aftapsysteem van de politie, Israël's konden meeluisteren'.

1b Kamer van Koophandel: Bedrijfsprofiel - Cognyte Netherlands B.V. (34139430).

1c Reuters: Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup, documents show.

129 b (new). 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 (AM 911, EPP)^{1a}. ***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 NSO Group were attracting a lot of public criticism, and the blacklisting by the US Department of Commerce hurt 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 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 (914, rapporteur).

Footnote:

1a <https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/>.

CA Belgium

Belgium

Paragraph 130 to 130 a (new)

Covered: 917 (Greens), 918 (rapporteur), 919 (EPP)

Falls:

130. In an interview with *The New Yorker*, a former Israeli intelligence official revealed that the Belgian police use Pegasus in their operations²⁵². In response, the Belgian police stated **they would** not ‘to 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 criminals²⁵³.

Footnote:

252 <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>.

253 <https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversielespionagetool-pegasus/10329450.html>.

130 a (new). *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^{1a}. 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 (917)^{1b}. 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 (919)^{1c}.*

Footnote:

1a <https://www.ft.com/join/licence/88bec95c-78fd-4030-9526-a95fbdeb9da8/details?ft-content-uuid=d9127eae-f99d-11e9-98fd-4d6c20050229>.

1b <https://www.vrt.be/vrtnws/nl/2021/09/17/pegasus-spionageware-op-de-telefoon-van-journalist-peter-verlind/>.

1c <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/>.

CA Germany and Use of Spyware

Germany

Paragraphs 131 to 132 d (new)

Covered: 920 (rapporteur), 921 (rapporteur), 922 (rapporteur), 923 (Left), 925 (EPP), 926 (rapporteur), 927 (Greens), 928 (rapporteur), 929 (Greens), 930 (Greens), 931 (Greens), 932 (rapporteur), 934 (rapporteur), 935 (rapporteur), 936 (Greens), 937 (Greens), 938 (rapporteur), 939 (rapporteur), 940 (rapporteur)

Falls: 924 (ECR), 933 (ECR Group)

131 -a (new). *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^{1a}. (920)*

Footnote:

1a European Parliament. Germany Hearing: <https://www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html>.

131 -b (new). *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 international terrorism and for the prevention of terrorist attacks^{1a}. 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^{1b}. 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^{1c} and stipulates the obligation for communication providers to cooperate with the state in hacking activities^{1d}. (921)*

Footnotes:

1a https://web.archive.org/web/20171008044948/https://www.gesetze-im-internet.de/bkag_1997/_20k.html.

1b https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0528.

1c <https://www.bundestag.de/dokumente/textarchiv/2021/kw23-de-verfassungsschutzrecht-843408>.

1d <https://netzpolitik.org/2020/staatstrojaner-provider-sollen-internetverkehr-umleiten-damit-geheimdienste-hacken-koennen/>.

131 -c (new). *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^{1a}. 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^{1b}. (922)*

Footnotes:

1a European Parliament. Germany Hearing.

1b 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

https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_Online_Durchsuchung_2020.pdf?__blob=publicationFile
<https://netzpolitik.org/2022/justizstatistik-2020-polizei-setzt-staatstrojaner-alle-zwei-wochen-ein/>.

131. 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 use²⁵⁴: access **to** all information (Online-Durchsuchung²⁵⁵) and access **to** only live communication (Quellen-TKÜ²⁵⁶). Since the original Pegasus software could access all information on a device, and not just live communication, its use by the BKA would **break** ~~violate~~ 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***^{256-a, 256a}. (923, *The Left*). The BKA therefore asked NSO to write a source code, so that Pegasus would only be able to access ~~only~~ what was allowed by law. Initially, NSO declined to do so²⁵⁷. Only after new negotiations ***did*** NSO ***agree*** ~~agreed~~, so the BKA ***acquired a modified version***²⁵⁸. ***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 camera meeting of the Innenausschuss in the Bundestag***^{258a}. 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*** ~~that~~ works in practice. The BKA has written a report about this modified version, which remains classified²⁵⁹. ***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***^{259a}. ***Despite two invitations to the PEGA Committee, the BKA has not been able to attend any hearings owing to scheduling issues*** (931).

Footnotes:

254

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

255 https://www.gesetze-im-internet.de/stpo/_100b.html.

256 https://www.gesetze-im-internet.de/stpo/_100a.html.

256-a 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](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf).

256a 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.

257 <https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197>.

258 <https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197>.

258a <https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197>.

259 <https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-pruflbericht-zur-pegasus-software/>.

259a 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/>.

131 a (new). 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^{1a} (926-927). 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)^{1b} (928, 929, 930).

Footnote:

1a <https://www.sueddeutsche.de/politik/pegasusprojekt-nso-pegasus-bundesnachrichtendienst-1.5433974>.

1b <https://dserver.bundestag.de/btd/19/322/1932246.pdf>.

Use of spyware Finfisher

132. In 2012 and 2013, both the German Federal Police BKA and the Berlin Police LKA independently purchased **FinSpy from (934) FinFisher spyware. Here too** ~~Also here~~, just ~~as~~ ~~like~~ 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 comply 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^{1a}. 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^{1b} (935-936).**

Footnotes:

1a 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](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf).

1b <https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/>.

132 a (new). In 2017, the Federal Minister of the Interior launched the Central Office for Information Technology in the Security Sector (ZITiS), for the facilitation of R&D for hacking tools by the government, as well as the purchase of hacking tools from commercial vendors^{1a} (938). 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^{1b}. Among other things, it was reported that, since 2019, it had met five times^{1c} with the Italian surveillance company RCS Lab, but there was no proof of the acquisition of a tool from RCS lab^{1d}. In addition, ZITiS met and evaluated spyware products of the Austrian firm DSIRF^{1e} and the Israeli firms Quadream^{1f} and Candiru^{1g} (937-939).

Footnotes:

1a https://www.zitis.bund.de/DE/Home/home_node.html.

1b <https://www.intelligenceonline.com/surveillance--interception/2022/04/06/after-finfisher-s-demise-berlin-explores-cyber-tool-options,109766000-art>.

1c Answer to a parliamentary question by The Left Party MP Martina Renner <https://dserver.bundestag.de/btd/20/038/2003840.pdf>.

1d <https://netzpolitik.org/2022/rcs-lab-hackerbehoerde-trifft-sich-mehrmals-mit-staatstrojaner-hersteller/>.

1e <https://dserver.bundestag.de/btd/20/001/2000175.pdf#page=12>.

1f <https://dserver.bundestag.de/btd/20/001/2000104.pdf#page=29>.

1g <https://dserver.bundestag.de/btd/20/003/2000327.pdf>.

132 b (new). 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, 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, Schmidbauer also contacted the President of ZITiS for a presentation of Intellexa. In addition, Schmidbauer 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 in the beginning of July 2022. The government did not comment on the appointments resulting from the controversial lobbying activities of Schmidbauer^{1a}. In 2021, Schmidbauer had also met Jan Marsalek, who is connected to DSIRF^{1b} (940).

Footnotes:

^{1a}

<https://www.tagesschau.de/investigativ/swr/predator-spionage-software-101.html>.

<https://dserver.bundestag.de/btd/20/050/2005061.pdf>.

^{1b} <https://www.tagesschau.de/investigativ/swr/wirecard-marsalek-schmidbauer-101.html>.

CA Malta

Malta

Paragraphs 133 to 133 e (new)

Covered: 941 (rapporteur), 942 (rapporteur), 943 (Greens), 944 (rapporteur), 945 (Greens), 946 (rapporteur), 947 (Greens), 948 (rapporteur), 949 (Greens), 950 (rapporteur), 951 (Greens)

133. Several key figures from the spyware trade have *either* registered a business on Malta or ~~they~~ have obtained Maltese passports, but it *appears seems* that they do not actually reside there, nor do their companies *appear seem* to be active. A few key personalities from the spyware trade have been identified so far. ~~÷ Tal Dilian, Anatoly Hurgin, Felix Bitzios, Stanislaw Szymon Pelczar, Peter Thiel~~ (941)

133 a (new). *Tal Dilian: Israeli citizen, formerly of the Israeli army, founder of Intellexa, living in Cyprus, acquired a Maltese passport in 2017^{1a}. He also co-owns a company on Malta called MNT Investments LTD^{1b}. (942-943)*

Footnotes:

1a 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>.

1b <https://mlt.databasesets.com/company-all/company/73006>; <https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/>.

133 b (new). *Anatoly Hurgin: Russian-Israeli citizen, former Israeli military engineer, acquired a Maltese passport in 2015^{1a}. He is the founder of Ability Ltd, which cooperated with NSO Group on Pegasus and handled the network side of NSO's operations^{1b}. 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^{1c}. Investigative journalist Daphne Caruana Galizia, who was later murdered in October 2017, wrote about him in August 2016^{1d}. 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^{1e}. Hurgin reportedly also owns a company in Lithuania, called UAB 'Communication technologies', in the area of 'connection and telecommunication services'^{1f}. (944-945)*

Footnotes:

1a <https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429>.

1b <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/>.

1c https://www.euractiv.com/section/all/short_news/mep-calls-out-malta-for-selling-passport-to-man-linked-to-pegasus-spyware/.

1d <https://daphnecaruanagalizia.com/2016/08/owner-israeli-phone-surveillance-hacking-software-intelligence-operation-buys-maltese-passport-citizenship/>.

1e <https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/>.

1f https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.

133 c (new). Felix Bitzios: Director of Malta-based company Baywest Business Europe Ltd^{1a}; formerly an owner and employee of Intellexa; involved in the Piraeus/Libra fraud case^{1b}; (946-947)

Footnotes:

1a <https://offshoreleaks.icij.org/nodes/55071906>.

1b <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>.

133 d (new). Stanislaw Szymon Pelczar: legal representative of Baywest Business Europe Ltd, registered in Malta; former administrator in Krikel; mentioned in the Paradise Papers^{1a}; (948-949)

Footnote:

1a <https://offshoreleaks.icij.org/nodes/55071906>.

133 e (new). Peter Thiel: German-born American citizen, acquired New Zealand citizenship in 2011 despite not residing there; applied for a Maltese golden passport in 2022 (shortly after the announcement of the joint start-up of Kurz and Hulio)^{1a}; founder of PayPal and of the controversial company Palantir (connected to the Cambridge Analytica scandal); sponsor of Donald Trump; first outside investor of Facebook; hired Sebastian Kurz (who recently set up business with Shalev Hulio, ex-NSO) as strategist^{1b}; (950-951)

Footnotes:

1a <https://www.nytimes.com/2022/10/15/technology/peter-thiel-malta-citizenship.html>.

1b <https://www.politico.eu/article/austria-former-chancellor-sebastian-kurz-palantir-technologies-silicon-valley-peter-thiel/>.

CA France

France

Paragraphs 134 to 135 g (new)

Covered: 953 (rapporteur), 954 (Greens), 955 (Left), 956 (Greens), 957 (rapporteur), 958 (Left), 959 (rapporteur), 960 (Greens), 961 (rapporteur), 962 (Greens), 963 (rapporteur), 964 (rapporteur), 965 (rapporteur), 966 (rapporteur), 967 (Greens), 968 (rapporteur), 969 (Greens), 970 (rapporteur), 971 (Greens), 972 (rapporteur), 973 (Greens), 974 (rapporteur), 975 (Greens), 976 (rapporteur), 977 (Greens), 978 (rapporteur), 979 (Greens)

Falls: 952 (ID)

Victims in France

134. In ~~the summer of~~ 2021, the Pegasus Project revealed several cases of attempted hacks by Pegasus in France.²⁶⁰ (953). ~~The~~ This leaked dataset included the telephone number of President Emmanuel Macron, as well as the phone numbers of 14 members of his cabinet²⁶¹ ²⁶². ~~The findings of forensic analyses by the French state intelligence services have confirmed that the telephones of several~~ *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* (953, 954) were infected with Pegasus spyware²⁶³. *The phone of Member of Parliament Adrien Quatennens was also infected*^{263a} (955).

Footnotes:

²⁶⁰ The Guardian. Pegasus spyware found on journalists' phones, French intelligence confirms.

²⁶¹ The Guardian. Spyware 'found on phones of five French cabinet members'.

²⁶² Euractiv. France's Macron targeted in project Pegasus spyware case.

²⁶³ The Guardian. Spyware 'found on phones of five French cabinet members'.

^{263a} 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.

134 a (new). 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 infection of the mobile devices belonging to the director of Parisian radio station TSF Jazz Bruno Delpont, former minister Arnaud Montebourg and investigative journalists Edwy Plenel, L  na  g Bredoux and an unnamed journalist from France 24 have been confirmed by France's computer security agency (Agence nationale de la s  curit   des syst  mes d'information)^{1a} (956, 957, 958). In addition, Claude Mangin – wife of Na  ma Asfari, a Saharawi political prisoner in Morocco – was also targeted with Pegasus^{1b} (957). Furthermore, the Paris-based defence lawyer of several Polisario Front activists for the Sahara cause, Joseph Braham, was also targeted with Pegasus^{1c} (956).

Footnotes:

^{1a} Haaretz. The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.

^{1b} Haaretz. The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.

^{1c} <https://www.middleeasteye.net/fr/entretiens/pegasus-espionnage-maroc-france-macron-sahara-occidental-braham-avocat-mangin-algerie>.

134 b (new). Morocco seems to be behind many of the attacks on both journalists and politicians in France,^{1a} 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 Jamaï who left Morocco in 2007^{1b} (960).

Footnotes:

^{1a} Radio France. *Projet Pegasus : le gouvernement et toute la classe politique française dans le viseur du Maroc.*

^{1b} <https://forbiddenstories.org/journaliste/hicham-mansouri/>; <https://forbiddenstories.org/journaliste/aboubakr-jamai/>.

134 c (new). 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^{1a}. The French Ministry of Foreign Affairs has denied talks with NSO Group^{1b} (959, 962).

Footnotes:

^{1a} MIT Technology Review. *NSO was about to sell hacking tools to France. Now it's in crisis.*

^{1b} MIT Technology Review. *NSO was about to sell hacking tools to France. Now it's in crisis.*

134 d (new). 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 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^{1a} (961)

Footnote:

^{1a} PEGA Committee Hearing. 9 January 2022.

134 e (new). 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, each operation authorised by the Prime Minister. If a victim 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 victim owing to the issue of this coming under national security confidentiality^{1a}. 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. (963)

Footnote:

^{1a} PEGA Committee Hearing. 9 January 2022.

134 f (new). According to an ISS World Brochure of 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 the presence of French spyware companies 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^{1a} (964).

Footnote:

^{1a} ISS World. Program Schedule for Year 2013.

Spyware companies in France

135. France is also home to **different the spyware industry companies, of which the most eminent are Nexa Technologies and Amesys (965)**. Nexa Technologies, part of Tal Dilian's Intellexa Alliance, is a French cyber defence and intelligence company, established in 2000²⁶⁴. Nexa Technologies is run by former managers of Amesys. Amesys was founded in 1979²⁶⁵ and is known for the sale of a programme called Cerebro, capable of tracking **the** electronic communications of its victims, **such as** like email addresses and phone numbers²⁶⁶.

Footnotes:

²⁶⁴ Bloomberg. Nexa Technologies Inc.

²⁶⁵ PitchBook. Amesys.

²⁶⁶ Le Monde. Vente de matériel de cybersurveillance à l'Egypte : la société Nexa Technologies mise en examen.

135 a (new). 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^{1a}. In 2014, Nexa Technologies had 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 of the Al-Sissi regime^{1b}. Eagle was deployed and maintained by Amesys from 2007 to 2011^{1c}. (966, 967)

Footnotes:

^{1a} ZDNet. Amesys and Nexa Technologies executives indicted.

^{1b} Trial International. Amesys (Nexa Technologies).

^{1c} ZDNet. Amesys and Nexa Technologies executives indicted.

135 b (new). 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^{1a}. Five Libyan victims were heard in the summer of 2013 and one Libyan victim 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^{1b}. (968-969)

Footnotes:

^{1a} Trial International. Amesys (Nexa Technologies).

^{1b} Trial International. Amesys (Nexa Technologies).

135 c (new). 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^{1a}. 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 (970-971).

Footnote:

^{1a} L'Obs. Amesys file un coup de main à l'agence en charge du fichier monstre.

135 d (new). 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^{1a 1b} (972-973).

Footnotes:

^{1a} Le Monde. Vente de matériel de cybersurveillance à l'Égypte : la société Nexa Technologies mise en examen.

^{1b} ZDNet. Amesys and Nexa Technologies executives indicted.

135 e (new). 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 in Libya and Egypt^{1a}. It is worrying that no less than 10 years had passed between the first complaint and the start of the court case. Meanwhile, Amesys had been able to continue its activity unhampered, including the abovementioned sale of surveillance technology to Egypt. (974-975)

Footnote:

^{1a} Amnesty. Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture.

135 f (new). 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 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^{1a} (976-977).

Footnote:

^{1a} L'Obs. Amesys file un coup de main à l'agence en charge du fichier monstre.

135 g (new). 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. (978-979)

CA Ireland

Ireland

Paragraphs 136 to 136 c (new)

Covered: 981 (EPP), 982 (rapporteur), 983 (Greens), 984 (rapporteur), 985 (Greens), 988 (rapporteur), 989 (Greens)

Falls: 980 (EPP), 986 (EPP), 987 (EPP)

136. Ireland has become the Member State where some of the main spyware companies involved in scandals have registered, **owing due** 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, have their headquarters in Ireland, and are 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 ~~reportedly~~ second wife, Sara Hamou, is **reportedly** named as director’ of both Thalestris and Intellexa²⁶⁷.

Footnote:

²⁶⁷ <https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/>.

136 a (new). *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^{1a}. (982, 983)*

Footnote:

^{1a} <https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/>.

136 b (new). *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^{1a}. (984, 985) There is no publicly known evidence of abuse of spyware in Ireland.*

Footnote:

^{1a} <https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-inside-the-predators-irish-lair/>.

136 c (new). *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 WiSpear and shut down in 2022, also had corporate ownership in Ireland^{1a}. (988, 989)*

Footnote:

^{1a} <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>.

136 d (new) *In January 2023, it was reported that the Oireachtas Committee on Justice is to examine the existence of companies in Ireland involved in the production of spyware following a letter 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.^{1a}*

Footnote:

^{1a} <https://www.irishtimes.com/politics/oireachtas/2023/01/29/justice-committee-to-investigate-controversial-spyware-technology-group-with-links-to-ireland/>.

136 e (new). *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. (981) 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^{1a}. (987)*

Footnote:

^{1a} <https://www.kildarestreet.com/wrans/?id=2022-12-15a.199&s=cyber+security#g201.r>.

CA Luxembourg

Luxembourg

Paragraphs 137 to 137 b (new)

Covered: 991 (rapporteur), 992 (Greens), 993 (S&D), 994 (S&D), 995 (rapporteur), 996 (Greens)

Falls: 990 (S&D)

137. 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 (990)**²⁶⁸. The fact that ~~Foreign Minister Jean Asselborn was initially only aware of two NSO entities based in the country~~²⁶⁹, and 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 Luxembourg allow companies to operate completely out of the public view **in Luxembourg**.

Footnote:

268 <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>.

137 a (new). *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^{1a}. 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 export licence^{1b}. 'Luxembourg will not, under any circumstances, tolerate that export operations from Luxembourg contribute 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^{1c}. 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^{1d}. 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^{1e}. (991, 992)*

Footnotes:

1a <https://www.luxtimes.lu/en/luxembourg/government-cannot-verify-pegasus-export-claims-616cead9de135b9236b1efcc>.

1b <https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e>.

1c <https://delano.lu/article/nine-nso-entities-in-luxembourg>.

1d <https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e>.

1e <https://www.luxtimes.lu/en/business-finance/pegasus-firm-nso-booked-most-sales-through-luxembourg-6303754ade135b9236e0870b>.

137 b (new). *In October 2021, Prime Minister Xavier Bettel confirmed that Luxembourg bought and used Pegasus, 'for reasons of state security'^{1a}. (995, 996)*

Footnote:

^{1a} <https://www.luxtimes.lu/en/luxembourg/tax-voting-rights-housing-watch-bettel-video-highlights-6176e835de135b923682378d>.

CA Italy

Italy

Paragraphs 138 to 138 b (new)

Covered: 997 (rapporteur), 998 (Greens), 999 (rapporteur), 1000 (Greens)

Falls:

138. So far, there have not been any reports on possible purchases of spyware by the Italian authorities. ***No high-level cases of spying have been reported, although the telephone number of*** ~~Apart from former Prime Minister and Commission President Romano Prodi~~ ***was found on the list published by the Pegasus Project²⁷⁰ (997)*** ~~who was spied upon with Pegasus by the Moroccan secret services, no high-level cases of spying have been reported.~~ As former UN Special Envoy for the Sahel, he could have been an interesting target for Morocco, considering his possible network with high-level figures in the Western Sahara or Algeria.

Footnote:

270 <https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/>.

138 a (new). Spyware companies Tykelab and RCS Lab have chosen Italy as their base for business. (998, 999)

138 b (new). 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 spyware RCS to attack political dissidents, journalists and human rights defenders. An inquiry launched by NGOs and UN investigators into export of RCS to Sudan eventually led the Italian authorities to impose a ‘catch-all’ provision of Italian export law owing to human rights concerns, 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, intelligence and law enforcement in Italy to position themselves as a national security asset and eventually pressured the Ministry of Economic Development into re-granting them a global licence for export^{1a}. (1000)

Footnote:

^{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/>.

CA Austria

Austria

Paragraphs 139 to 139 b (new)

Covered: 1001 (EPP), 1002 (rapporteur), 1003 (Greens), 1004 (S&D), 1005 (S&D), 1006 (rapporteur), 1007 (Greens), 1008 (S&D), 1009 (S&D), 1010 (S&D)

Falls:

139. In response to written questions by ~~the National Council of Austria (the lower house) of the Austrian Parliament, former Minister of Interior Karl Nehammer~~ **the Austrian Federal Government** stated that Austria has not been a client of NSO²⁷¹ **(1001)**. 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.

Footnote:

271 Responses by former Minister of the Interior Karl Nehammer to Member of National Council Nikolaus Scherak, 22 September 2021, Reference 2021-0.580.421.

139 a (new). *Following his resignation, Kurz was subsequently recruited as global strategist for Thiel Capital, owned by billionaire Peter Thiel^{1a}. In October 2022, Kurz and Shalev Hulio (founder of NSO Group) launched a cybersecurity firm called Dream Security^{1b} (1002, 1003, 1010). Although Hulio had stepped down as NSO Group CEO in August 2022, Dream Security and NSO have close ties through various personalities 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^{1c}.*

Footnotes:

^{1a} <https://www.bloomberg.com/news/articles/2021-12-30/billionaire-thiel-gives-austria-s-former-wunderkind-a-job>.

^{1b} <https://www.spiegel.de/netzwelt/web/sebastian-kurz-und-ex-nso-chef-gruenden-it-sicherheitsfirma-dream-security-a-4482132c-9faf-4be3-927a-86560ba28670>.

^{1c} <https://www.timesofisrael.com/former-nso-ceo-ex-chancellor-of-austria-establish-new-cybersecurity-startup/>.

139 b (new). *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^{1a} (1004). In October 2022, the Federal Ministry of Labour and Economic Affairs said it was not aware of any applications for export licences by DSIRF (1005), and that no export applications for 'intrusion software' had been made in the last 10 years^{1b} (1008). 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 (1006, 1007, 1009).*

Footnotes:

^{1a} 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.

^{1b} https://www.parlament.gv.at/dokument/XXVII/AB/11698/imfname_1473647.pdf.

CA Estonia & Lithuania

Estonia

Paragraphs 140 to 140 a (new)

Covered: 1011 (rapporteur), 1012 (Greens)

Falls:

140. Estonia has reportedly also been interested in purchasing NSO Group's Pegasus spyware. In 2018, initial negotiations between Estonia and NSO Group took place, leading Estonia to make a down payment on the **USD** 30 million ~~dollars~~ deal for the surveillance software^{1a}.

140 a (new). *However, one year later, a Russian defence official notified Israel about Estonia's intention to use the Pegasus spyware on Russian phone numbers. This information led the Israeli Ministry of Defence to block Estonia from spying on any Russian devices worldwide, stating that the deal would be harmful to Israeli-Russian relations^{1a}. The case of Estonia underlines that Pegasus spyware is not just a surveillance weapon, but also serves as political currency in diplomatic relations (1011)*

Footnote:

1a <https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html>.

1a The New York Times. [*Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia.*](#)

Lithuania

Paragraphs 141

Covered: 1013 (EPP)

141. ***A Lithuanian company UAB 'Communication technologies', operating in the area of 'connection and telecommunication services', is owned by Anatoly Hurgin, a Russian-Israeli citizen, former Israeli military engineer and co-developer of Pegasus together with NSO²⁷³, reportedly owns a company in Lithuania, called UAB 'Communication technologies', in the area of 'connection and telecommunication services. He also acquired a Maltese golden passport in 2015²⁷⁴. (1013)***

Footnote:

273 https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.

274 <https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-falsedeclaration.744429>.

CA Bulgaria

Bulgaria

Paragraph 142

Covered: 1014 (S&D), 1016 (rapporteur), 1017 (Greens), 1018 (EPP), 1019 (rapporteur), 1020 (Left), 1022 (rapporteur), 1024 (Greens), 1025 (rapporteur), 1026 (Greens), 1028 (rapporteur), 1029 (Greens)

142. In Bulgaria, export controls and export licences for products that are categorised as ‘dual-use’, as outlined in the EU Dual-Use Regulation, are controlled by the Ministry of Economy, more particularly by the Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction²⁷⁵. The current Minister of Economy and Industry is Nikola Stoyanov²⁷⁶. ~~Up until today,~~ The Bulgarian authorities deny having granted export licences to NSO Group *or its subsidiaries*²⁷⁷. ~~However Yet,~~ former private equity owner of NSO Group Novalpina Capital emphasised that NSO products are being exported from the EU from both Cyprus and Bulgaria^{278 279 280}. *Furthermore, media publications claim that some of the servers of the network infrastructure over which Pegasus attacks are conducted are located in a Bulgarian datacentre, owned by a Bulgarian company, in turn owned by NSO Group, Circles Bulgaria and Magnet Bulgaria, which have received export licences from the authorities (1014, 1024, 1025, 1026). From Bulgaria, this subsidiary of NSO Group provides the Cypriot subsidiaries of research and developments services and export network products to governments*^{280a}. *(1016-1017). These two claims are contradictory. Magnet is currently dormant, but Circles is currently still active and has received an export licence that is valid until 25 April 2023*^{280b}. *(1025, 1026).*

142 a (new). 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 and the investigation is currently ongoing^{280c}. *In January 2022, in the case of Ekimdzhiev and Others v. Bulgaria, the ECtHR found that the existing laws in Bulgaria on the secret surveillance and the 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*^{280d}. *(1014, 1018, 1028)*

Footnotes:

275 Republic of Bulgaria. Ministry of Economy and Industry. Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction.

276 Council of Ministers of the Republic of Bulgaria.

277 POLITICO. Pegasus makers face EU grilling. Here’s what to ask them.

278 Amnesty International. Novalpina Capital’s response to NGO coalition’s open letter (18 February 2019).

279 Access Now. Is NSO Group’s infamous Pegasus spyware being traded through the EU?

280 <https://www.business-humanrights.org/en/latest-news/noalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/>.

^{280a} Amnesty International. Operating From the Shadows: Inside NSO Group’s Corporate Structure.

^{280b}

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.

^{280c} <https://bnr.bg/en/post/101599684/sofia-city-prosecutor-s-office-investigates-possible-use-of-pegasus-spyware-in-bulgaria>.

^{280d} 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>.

Compromises EU Institutions

Covered: 1032 (rapporteur), 1033 (Greens), 1034 (Greens), 1035 (rapporteur), 1036 (rapporteur), 1037 (Greens), 1038 (rapporteur), 1039 (Greens), 1041 (rapporteur), 1042 (Greens), 1043 (rapporteur), 1045 (EPP)
Falls: 1040 (ECR), 1044 (EPP), 1046 (EPP)

I.G. EU Institutions

Targeting of the European Commission

143. ~~Following the Forbidden Stories and Amnesty International's revelations in July 2021, the Commission set up a 'dedicated team of in-house experts', which launched an internal investigation on 19 July 2021, with the aim 'to verify whether Pegasus had targeted devices of Commission staff and members of the College'²⁸³. On 23 November 2021, Apple sent official notifications to the devices of Commissioner Reynders and 'additional Commission staff', that they were 'targeted by state-sponsored attackers' and their devices might have been compromised²⁸². On 11 April 2022, Reuters reported that Didier Reynders, Commissioner for Justice, and at least four Commission staff members had been targeted with Pegasus software in November 2021²⁸³. ***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^{283a}.***~~

283 <https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/>.

283a 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

143 a (new). 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. Already on 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'^{1a}. 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.

143 b (new). In the course of the investigation, the Commission communicated that, 'neither ... before or after this date [23 November]' 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^{1b}. (1032, 1033)

Footnote:

1a Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 July 2022.

1b Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.

143 c (new). 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’^{1a}. Unofficial reports of more than 50 detected infections have not been confirmed by the Commission.

143 d (new). 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^{1a}, 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 (1034, 1035), 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’^{1b}.

Footnotes:

1a <https://pro.politico.eu/news/148627>

1b Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022,

143 e (new). 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.

143 f (new). 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 ‘Endpoint Detection and Response’ solution, on all Commission phones, and engages in continuous cooperation with CERT-EU^{1a}, 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. (1042-1043)

Footnote:

1a Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.

143 g (new). *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 ‘Notifications 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^{1a}.*

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’, but it fails to explain how Commissioners and Commission staff could plausibly constitute a risk to national security. (1038, 1039).

Footnotes:

1a Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 September 2022.

1b Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 July 2022.

143 h (new). *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.*

~~144. According to the Commission, ‘it is impossible to attribute these indicators to a specific perpetrator with full certainty.’ The Commission holds that it cannot elaborate on the investigation’s present day findings, as ‘they would reveal to adversaries the Commission’s investigation methods and capabilities, thus seriously jeopardizing the institution’s security’. The common, overarching topic that two of the known targeted Commission officials, Commissioner Reynders and a cabinet member of Commissioner Věra Jourová²⁸⁴, are dealing with is the rule of law. In response to PEGA’s question about a possible correlation, the Commission states 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’²⁸⁵.~~

Footnotes:

~~284 <https://pro-politico.eu/news/148627>~~

~~285 Response letter by Commissioners Hahn and Reynders to the PEGA committee – 9 September 2022,~~

~~145. In its interaction with the PEGA committee, the Commission repeatedly explained that the hack of Commissioner Reynders’s device with Pegasus software did not succeed, seemingly downplaying the gravity of a Commissioner being targeted. However, any attempted hack – successful or not – of (a member of) the Commission is a very grave political fact that affects the integrity of the democratic decision-making process.~~

Cybersecurity measures

~~146. Following the attempted hack of Commissioner Reynders’s phone and the indicators of compromise on several devices of Commission staff, the Commission deployed a mobile ‘Endpoint Detection and Response’ (EDR) solution on all corporate phones in September 2021.~~

Targeting of members of the European Council, the Council and the Commission

Targeting of former Greek Commissioner and representatives in the Council

-147 a (new). 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.

-147b. 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.

147. ~~On 6 November, 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 devices²⁸⁶, ~~including Dimitris Avramopoulos, European Commissioner from 2014-2019 and~~ **Néa Dimokratia politician, 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 happened** ~~he was targeted~~ while he was member of the College, or who was behind **them**, but ~~considering~~ the long list of targeted people **includes** many Greek politicians from both the governing party and the opposition **(1045)**. ~~including many politicians from both Néa Dimokratia and opposition, the most plausible hypothesis is that the orders came from the entourage of the Prime Minister~~

Footnote:

286 *Documento*, edition 6 November 2022.

148. **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.**

~~This case therefore demonstrates that (former) Commissioners, including their communications with colleagues, can be targeted for domestic political reasons at any given moment from within their Member States. Moreover, among the list of targets published by Documento, there are several current government ministers, including the ones of Foreign Affairs and Finance. These ministers are also members of the Council, deciding on EU foreign and finance policy. Therefore, a single infected phone could also serve to wiretap in real-time all Commission and Council meetings.~~

Compromises on Third Countries

148 a (new). The following section will highlight to what extent the use of the Pegasus or 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, to what extent 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 such 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.

148 aa (new). Among 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 geopolitics of spyware. In addition, a hearing in August 2022 was partly dedicated to Rwanda, with remarks from Ms Carine Kanimba, who was a target of Pegasus.

Covered: AM 13 (S&D), AM 1030 (Left), AM 1031 (Left), AM 1054 (Greens), AM 1056 (Greens), AM 1057 (Greens), AM 1058 (Greens), AM 1062 (Greens), AM 1063 (Greens), AM 1064 (Greens),

Fall: AM 1059 (Greens), AM 1060 (Greens), AM 1061 (Greens)

1. Israel (AM 1054)

148 ab (new). The PEGA Committee visited Israel in July 2022 with the main purpose to meet with the manufacturer of the Pegasus spyware, the NSO Group, which is an Israeli-based company. The PEGA delegation learned that NSO Group has sold spyware to fourteen EU governments, using export licenses 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 has underlined the ineffectiveness of the safeguards against 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 the future.

148 b (new). The geopolitical and security situation that Israel has faced have prompted the government and private sector to develop intelligence gathering tools that would expand its cybersecurity capabilities, especially with regards to its defense. Over the years, Israel has become one of the leading producers of advanced surveillance technologies and spyware in the world as they have lots of 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”. This is also confirmed by news reports, where experts

confirm the usefulness of Pegasus in forging diplomatic relations, ie with Gulf states^{1a}. (AM 1056)

Footnotes:

1a <https://www.france24.com/en/livenews/20210719-pegasus-scandal-shows-risk-of-israel-s-spy-tech-diplomacyexperts>

148 c (new). In addition to strategic domestic reasons, Israel has successfully promoted itself as an innovative startup nation including firms with the most sophisticated technology in the field, such as NSO, Cellebrite, Candiru, QuaDream and Intellexa. The industry's collective sales are estimated to be at least \$1 billion annually^{1a}, amounting to about 0.6 per cent of Israel's exports^{1b}. 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 percent of the 2,300 people who founded Israel's 700 cybersecurity companies were former employees of the Israeli Defense Forces' intelligence units". One of its most prominent figures is Intellexa owner and founder Tal Dilian (see Chapter on Intellexa and Tal Dilian)^{1c}. (AM 1057)

Footnotes:

1a. <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>

1b. <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.>

1c. <https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000>

148 d (new). Israeli spyware companies have sold surveillance technology throughout the world including to EU member states as well as to authoritarian Gulf countries. According to Haaretz newspaper, the sale of Pegasus was used as diplomatic bargaining chip and facilitated negotiations for establishing formal diplomatic ties under the so called Abraham Accords with Morocco, Bahrain, and formally also the United Arab Emirates^{1a}. (AM 1030, AM 1058). The sale of spyware to authoritarian regimes has been criticized, 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 light of Israel's planned judicial overhaul, many Israeli tech companies are reportedly incentivized by Greece, Cyprus and Portugal to relocate their businesses to the countries in question. According to media reports, the three countries allegedly offer Israeli tech companies tax breaks and Greece reportedly provides fast-tracked citizenship^{1b}.

Footnote:

1a. 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-it-for-his-downfall/0000017f-e941-dc91-a17f-fdcd55c80000>

1b. <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>

148 e (new). *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 also NSO has benefited from^{1e}. As a result, countries acquiring “field trained” spyware from Israel contribute 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 EU foreign and security policy agenda regarding the support of human rights and democracy^{1f}. (AM 1062)*

Footnotes:

1a. PEGA Mission to Israel 18-20 July 2022.

1b. In line with most findings of the 2021 Annual Report on the “Application of the EU Charter of Fundamental Rights ‘Protecting Fundamental Rights in the Digital Age’”, the EU is obliged to facilitate the work of HRDs online.

148 f (new). *NSO’s Pegasus spyware has been used to target Palestinian civil society, among them six Palestinian human rights defenders^{1a}. In the cases of Ubai AlAboudi, executive director of Bisan Center for Research and Development and Salah Hammouri, a dual French national, lawyer and field researcher at Addameer Prisoner Support and Human Rights Associations, 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. The case of surveillance of Palestinian human rights defenders is yet another proof for lack of enforcement of NSO’s Human Rights Policy^{1b}, which the company has used to boost its legitimacy and credibility when selling to EU Member States. (AM 1031, AM 1063)*

Footnotes:

1a. <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/>

1b. <https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/>

148 g (new). *It shall be noted that the Commission 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 of 09 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”. (AM 1064)*

Covered: AM 896 (Greens), AM 1015 (Left), AM 1021 (Left), 1065 (Greens), AM 1066 (Greens), AM 1067 (Greens), AM 1068 (Greens), AM 1069 (Greens), AM 1070 (Greens),

Fall: AM 1027 (Left)

2. Morocco (AM 1065)

148 h (new). *Multiple news reports have documented the alleged widespread use of spyware by Morocco. With a licence for about 10.0000 phone numbers, Morocco can be considered as one of NSO's biggest Pegasus clients^{1a}. Morocco has refuted the accusations tied to the Pegasus Project as "erroneous". (AM 1066). In December 2020, a CitizenLab report revealed that Morocco is one of the 25 customers of Circles, a subsidiary of NSO Group (AM 1015)^{1b}.*

Footnotes:

1a. <https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara>

1b. <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>

148 i (new). *The revelations also demonstrated that within the country, surveillance with spyware has allegedly been used to hack and subsequently intimidate journalists and activists^{1a}. In a recent resolution on the surveillance and imprisonment of investigative journalist Omar Radi, the European Parliament has condemned the Moroccan government's sustained judicial harassment against journalists and urged the country "to end their surveillance of journalists, including via NSO's Pegasus spyware"^{1b}. One of the targeted individuals, Ignacio Cembrero, an investigative journalist at the Spanish newspaper El Confidential, appeared before the Committee on 29 November. He was made aware of the hacking of his phone after text messages between him and the Spanish government were published in a Moroccan newspaper. Upon the request of a Spanish court to cooperate, Israeli authorities have refused to supply further information to aid the case (AM 1067).*

Footnotes:

1a. <https://daraj.media/en/76202/>

1b. European Parliament resolution of 19 January 2023 on the situation of journalists in Morocco, notably the case of Omar Radi (2023/2506(RSP)) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0014_EN.html

148 j (new). *Morocco also persecuted Moroccan journalists in French exile Hicham Mansouri and Aboubakr Jamaï^{1a} as well as supporters of the Western Sahara, namely Paris-based defence lawyer Joseph Breham and Belgium-based Sahrawi Human rights defender El Mahjoub Maliha^{1b}. (AM 1021, AM 1068)*

Footnotes:

1a. Forbidden Stories. <https://forbiddenstories.org/journaliste/hicham-mansouri/>, <https://forbiddenstories.org/journaliste/aboubakr-jamai/>

1b. <https://www.middleeasteye.net/fr/entretien-s/pegasus-espionnage-maroc-francemacron-sahara-occidental-brehamavocat-mangin-algerie>

148 k (new). *Morocco has launched several legal proceedings against 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, Paris Correctional Court dismissed the cases as inadmissible and the Moroccan authorities appealed the decision. In Spain, the Moroccan authorities filed a case against journalist Cembrero on a Medieval Age-old clause in the Penal Code of “an act of bragging”. The case is ongoing and has been denounced as seeking to intimidate Cembrero and others from reporting on Morocco’s use of the spyware^{1a}. (AM 896, AM 1069)

Footnote:

1a. <https://www.middleeastmonitor.com/20220705-morocco-files-lawsuit-against-spain-journalist-who-reported-use-of-pegasus-spyware/>

148 l (new). According to a news report, prior to its widespread use of Pegasus, Morocco was reportedly also client of at least three European spyware providers, the French companies Amesys and Vupen^{1a}, as well as the Italian Hacking Team. According to confidential documents, Morocco was the third largest client of the Italian company and paid more than 3 million euros over six years to acquire Hacking Team’s RCS software for its domestic High Council for National Defence (CSDN) and the Directory of Territorial Surveillance (DST)^{1b}. With the help of the spyware, multiple high-level UN departments and services have been surveilled (AM 1070).

Footnotes:

1a. <https://moroccomail.fr/2022/09/21/morocco-used-hacking-team-to-spy-on-the-un/>

1b. <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/>

148 m (new). 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 (FrenchLebanese MSAB’s spyware “XRY” and US-based Oxygen Forensics spyware called “Detective”)^{1a}. 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 also teach the police how to extract information from social media profiles via social hacking^{1b}. Contrary to Pegasus, the spywares mentioned can only enter the device physically and do not leave any traces of its use. The report outlines multiple cases, among them journalists and activists, in which smartphones have been taken away from targets and returned with hints towards possible infiltration afterwards. Despite the fact that there is no possibility to verify whether the spyware has been used properly by third parties, there were no indications that the Commission verified the proper use of the supplied technologies. Similar to a complaint to the EU Ombudsman on the funding for surveillance technologies under the EUTFA programme (see chapter below), no impact assessment have been conducted by the Commission to map possibly misuse of the supplied technologies. The Commission has stated that it is up to the user, Morocco, to deploy the spyware responsibly and according to the contractual agreement (for outlined purposes only)^{1c}.

Footnotes:

- 1a. <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>
1b. <https://privacyinternational.org/longread/4289/revealed-eu-training-regimeteaching-neighbours-how-spy>
1c. <https://disclose.ngo/en/article/how-theeu-supplied-morocco-with-phonehacking-spyware>

Covered: AM 1072 (Greens), AM 1073 (Greens),

Fall: AM 15 (ECR), AM 1074 (Greens)

3. Other third countries (AM 1072)

148 n (new). Globally, at least 75 countries have purchased and/or used spyware, including repressive regimes^{1a}. Human rights organizations 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^{1b}. (AM 1073).

Footnotes:

1a. Carnegie Endowment for International Peace (11 January 2023): Global Inventory of Commercial Spyware & Digital Forensics <https://carnegieendowment.org/programs/democracy/commercialspyware>

1b. Forensic Architecture/ Amnesty International / The Citizenlab: Digital Violence <https://www.digitalviolence.org/#/>

Covered: AM 1082 (Greens), AM 1084 (Greens), AM 1085 (Greens), AM 1086 (Greens), AM 1087 (Greens)

Fall: AM 1076 (Greens), AM 1077 (Greens), AM 1078 (Greens), AM 1079 (Greens), AM 1080 (Greens), AM 1081 (Greens), AM 1083 (Greens),

4. EU member states' complicity as NSO group clients for Pegasus abuse in third countries (AM 1082)

148 o (new). 14 non-EU country authorities are most likely responsible for many such cases where targeted people have been identified and where the infection was technically proven. This is the case for El Salvador, Mexico, Thailand, Morocco, India, Rwanda, Saudi Arabia, Bahrain, Jordan, Kazakhstan, Togo, the UAE, Israel and Azerbaijan^{1a} (AM 1084).

Footnote:

1a. <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/>

148 p (new). The so-called Pegasus Project, a collaboration by more than 80 journalists from 17 media 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 software 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 well as his son, Abdullah, who was also selected as a target along with other family members in Saudi Arabia and the UAE^{1a}. (AM 1085)

Footnote:

1a. Amnesty International (19 July 2021) Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally <https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/>

148 q (new). In addition, the Pegasus Project has documented that journalists have been frequent targets of the Pegasus spyware: In Mexico, journalist Cecilio Pineda's phone was selected for targeting just weeks before his killing in 2017. Pegasus has been used in Azerbaijan, a country where only a few independent media outlets remain. More than 40 Azerbaijani journalists were selected as potential targets according to the investigation. Amnesty International's Security Lab found the phone of Sevinc Vaqifqizi, a freelance journalist for independent media outlet Meydan TV, was infected over a two-year period until May 2021. In India, at least 40 journalists from nearly every major media outlet in the country were selected as potential targets between 2017-2021. Forensic tests revealed 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^{1a}. (AM 1086)

Footnote:

1a. Amnesty International (19 July 2021) Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, <https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/>

148 r (new). Human rights defenders continue to be frequently targeted, including by the authorities of the following countries: Mexico, El Salvador, Morocco, Rwanda, Israel, Jordan, Saudi Arabia, Bahrain, United Arab Emirates, India and Kazakhstan, Indonesia and Belarus^{1a}. In 2021 Frontline Defenders published a report documenting the targeted surveillance of human rights defenders including in India. In June 2018 sixteen human rights defenders were jailed under anti-terror law, in what is known as the Bhima Koregaon case, which relates to the violence that took place in Bhima Koregaon. One of the defenders, 84 year old Jesuit priest, Stan Swamy, died in custody in July 2021^{1b}. A digital forensics investigation found that 'evidence' relied on by the prosecution against the group had been planted through Pegasus spyware onto IT devices of human rights defenders Rona Wilson and Surendra Gadling and that there was no evidence that the defenders interacted^{1c}. (AM 1087)

Footnotes:

1a. <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/>

1b. Frontline Defenders (2 December 2021): Action needed to address targeted surveillance of human rights defenders <https://www.frontlinedefenders.org/en/statement-report/action-needed-address-targeted-surveillance-human-rightsdefenders>

1c. The Wire (17 December 2021) Rona Wilson's iPhone Infected With Pegasus Spyware, Says New Forensic Report, <https://thewire.in/rights/rona-wilsonpegasus-iphone-arsenal>

Compromises Spyware Industry

COMP Paragraph 149

Covered: AM 1090 (Greens), AM 1091 (Rapporteur), AM 1092 (Greens)

Fall: AM 1088 (Mandl), AM 1089 (ID)

149. The European Union is an attractive place for the trade in surveillance technologies and services, including spyware tools. On the one hand, there are the Member State governments as potential customers. On the other hand, the notion of being ‘EU regulated’ serves as **the benchmark** ~~a quality label~~, 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** ~~they can be easily circumvented as~~ Member States **circumventing these and seeking** to get a competitive advantage with ~~deliberate lax~~ **improper** national implementation. ~~and Furthermore,~~ enforcement by the European Commission **is has often been inadequate** ~~weak and superficial~~. Indeed, each time the regime for export licenses was tightened in Israel, several companies moved their export departments to Europe, in particular Cyprus^{287 288}. Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.

149 a (new). 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. First reports on the roles of these companies in monitoring journalists and crushing dissent became known over ten years ago when with the advent of protest movements known as the Arab Spring contracts of these companies started emerging from offices of secret police^{288a}. (1090)

149 b (new). The spyware industry has an obfuscating structure, including an entanglement of persons, locations, connections, ownership structures, letterbox companies, ever changing corporate names, money flows, government proxies and middlemen, tycoons and governments. (1091, 1092)

Footnotes:

287 Makarios Drousiotis. *State Mafia*. Chapter 6. Published 2022.

288 Haaretz. Cyprus, Cyberspies and the Dark Side of Israeli Intel

288a. PEGA Hearing of 30.08.22 on impact of spyware on EU Citizens <https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/>

COMP Paragraph 150

Covered: AM 1094 (Rapporteur), AM 1096 (Greens), AM 1097 (Rapporteur), AM 1099 (Greens)

Fall: AM 1093 (ID), AM 1098 (Greens)

150. In many cases, the nickname ‘mercenary spyware’ seems to be accurate. ***As the number of persons illegally targeted demonstrates, the sector many companies does not have very high-lacks fall behind with regards to ethical standards, often*** selling to the bloodiest dictatorships and wealthy non-state actors with unfriendly intentions. The list of victims of spyware tells the real story, not the hollow human rights pledges in the brochures of the vendors. 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 Russian activists. However, in October 2022 there are signs that Cellebrite is still being used by the Russian authorities Putin²⁸⁹. It is a lucrative, booming and shady dubious ambiguous market, attracting a lot of cowboys. Still, they many spyware companies get to sell their products to democratic governments in the US and the EU, which grants a veneer of respectability. Nonetheless, despite the claims that the use of spyware is entirely legitimate and necessary, governments are remarkably shy 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 fairs of the arms industry.

Footnote:

289. <https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-usingisraeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000>

150 a (new). Next to 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 waterproof evidence, as this trade leaves no few traces. Greek newspaper Documento claims to have evidence that the software is being sold on the black market – for up to \$50 million – not only to governments and counter-terrorism agencies, but also to private individuals^{1a}. Another Greek newspaper, To Vima, reported that Predator was sold to 34 customers from Greece^{1b}. Leaked documents show a pirated version of the product that was officially sold only to governments, at a price of \$8 million, an amount that included training the agents who will use the program, 24-hour technical support and monitoring of the victim's social media accounts^{1c}. (1094, 1096).

150 b (new). 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. (1097, 1099).

Footnotes:

1a Documento. Documento's 'Predator' revelations on Euractiv – Europol's intervention calls for Dutch MEP

1b To Vima. Interceptions “Spy software has 34 customers.”

1c <https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/>

COMP Paragraph 151

Covered: AM 1100 (S&D), AM 1101 (Greens), AM 1102 (Rapporteur), AM 1103 (Rapporteur), AM 1104 (Rapporteur)

Fall:

Vulnerabilities

151. Without vulnerabilities in software, 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 well²⁹⁰. 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.

Footnote:

290 Ot van Daalen, intervention in PEGA 27 October 2022; EDRI Paper: Breaking encryption will doom our freedoms and rights <https://edri.org/wpcontent/uploads/2022/10/EDRI-Position-Paper-Encryption.pdf>
<https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu>

151 a (new). *Vulnerabilities therefore need to be disclosed and fixed as soon as possible. However, current EU law encourages the opposite of disclosure. In 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 for selling the knowledge of the vulnerability to a private broker, in return for high remunerations. (1100, 1101, 1102).*

151 b (new). *This practice has generated a lively and lucrative trade in vulnerabilities. However, it is not just brokers in zero-days vulnerabilities looking for vulnerabilities: security and law enforcement authorities stockpile vulnerabilities as well, sometimes found by their own experts, sometimes acquired from brokers. If vulnerabilities go unreported, they are not patched, thus leaving IT systems weakened and the users unprotected. This allows the use of spyware to continue. (1103, 1104).*

COMP Paragraph 152

Telecom Networks

Covered: AM 1105 (Rapporteur), AM 1106 (Greens)

Fall: AM 1107 (Greens)

152. 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, quantum computing, but at the same time we are using and strongly relying on an international telecommunication protocol called SS7. This protocol was developed in 1975 and it is still used today. This system controls how telephone calls are routed and billed, and it enables advanced calling features and Short Message Service (SMS)²⁹¹. Via the SS7 network you have the capability to intercept phone calls, SMS and identify geo-location and also to infect a victim with spyware, such as Pegasus, Predator etc.²⁹²

Footnotes:

291 <https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7 was first adopted as,up to and including 5G.>

292 <https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453>

152 a (new). *The risk of abuse by the telecom providers of access to these networks is high. We have several documented misuses, where access points (global titles) were leased to companies that were monitoring and intercepting communications of targets based on the man-in-the-middle attacks. They were also harvesting geo-location data, meta-data for their*

own economical purposes. A global title is an address used for routing messages within Signaling System Number 7 (SS7). It can be compared to an IP address, in that the global title refers to an address within the telecommunications system^{1a}. This is also, according to a whistleblower, the reason why the access to the SS7 network in the US was so interesting for NSO, that they were trying to buy their access^{1b}. Telecom providers are deliberately keeping these low industry standards in order to provide an easier access to local state enforcement agencies. (1105, 1106).

Footnotes:

1a. <https://www.gms-worldwide.com/glossary/global-title/>

1b. <https://www.theguardian.com/news/2022/feb/01/nso-offered-us-mobile-security-firm-bags-of-cash-whistleblower-claims>

COMP Paragraph 153

Covered: AM 1108 (Rapporteur), AM 1109 (Greens), AM 1110 (Rapporteur), AM 1111 (Greens), AM 1112 (Rapporteur), AM 1113 (Greens),

Fall:

THE NSO GROUP

153. 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 crime²⁹³. Pegasus spyware is the best known product of the NSO Group. It was brought onto the global market in 2011^{294 295}.

Footnotes:

293 NSO Group. *About us*.

294 NYTimes. *The Battle for the World's Most Powerful Cyberweapon*.

295 Hulio S., *NSO Never Engaged in Illegal Mass Surveillance*, *The Wall Street Journal*, 24 February 2022

153 a (new). Since its launch in 2010, the NSO Group has had 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. The NSO Group has however stated in their Transparency and Responsibility report of 2021 that Bulgaria and Cyprus are both export hubs^{1a}. According to Amnesty International, the Dutch entities (liquidated on December 22, 2016) functioned in the sector of financial holdings and Q Cyber Technologies as based in Luxembourg was active as a commercial distributor responsible for the issuance of invoices, signing of contracts and receiving payments from customers. In addition, Westbridge Technologies as registered in the US may have facilitated the company's US sales^{1b}. (1108, 1109).

Footnotes:

1a. NSO Group. *Transparency and Responsibility Report 2021*.

1b. Amnesty International. *Operating from the shadows. Inside NSO Group's corporate structure*.

153 b (new). NSO reportedly had revenues of \$243 million in 2020^{1a}. However, following the revelations by the Pegasus Project, the company faced several difficulties. Lawsuits filed by Apple^{1b} and Meta^{1c} against the company, 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 group, have led to a

severe decline in profit. Reportedly, the NSO Group's debt at one point even reached 6.5 times its normal revenues for a year^{1d}. (1110, 1111)

Footnotes:

1a. Haaretz. NSO Is Having a Bad Year - and It's Showing.

1b. Apple. Apple sues NSO Group to curb the abuse of state-sponsored spyware.

1c. Bloomberg Law. NSO Loses Latest Challenge to Meta Lawsuit Over Whatsapp Spyware.

1d. Bloomberg. Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop.

153 c (new). 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 twenty-two end-users in fourteen EU Member States, using marketing and export licenses issued by Israel. Contracts with end-users in two Member States were subsequently terminated^{1a}. It has not been confirmed which Member States are included in the list of fourteen, nor which two countries were removed. However, it could be assumed the two are Poland and Hungary. (1112, 1113).

Footnote:

1a. Answers provided by NSO Group to PEGA secretariat following hearing, 20 July 2022.

COMP Paragraph 154

Covered: AM 24 (S&D), AM 1114 (Rapporteur), AM 1115 (Greens), AM 1116 (Rapporteur), AM 1117 (Greens), AM 1118 (Rapporteur), AM 1119 (Greens), AM 1120 (Rapporteur), AM 1121 (Greens),

Fall:

Corporate structure, transparency and due diligence

154. On 25 January 2010, the NSO Group launched its first company in Israel. This company was registered under the name of NSO Group Technologies Limited. The NSO Group is both the name of the first registered company, as well as the umbrella term for the various established companies in other jurisdictions. This first established company is the owner of the NSO Group trademark²⁹⁶.

Footnote:

296. Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

154 a (new). 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 USA, the Netherlands and Luxembourg. During the Francisco Partners years between 2014 and 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 has denied tens of millions of dollars' worth of sales that would have otherwise be approved of under legal requirements^{1a}. (1114, 1115)

Footnote:

1a. Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

154 b (new). Francisco Partners sold their entire ownership interest, including that of the subsidiaries, on February 14, 2019 to Novalpina Capital. 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 human rights records of potential customers^{1a}. (1116, 1117).

Footnote:

1a. PEGA Committee Hearing with NSO, 21 June 2022;

154 c (new). In line with the End Use/User Certificate after the tightening of the Israeli export regime, the NSO Group has introduced a Human Rights Policy and a Human Rights Due Diligence (HRDD) procedure. As described in the NSO Group's Transparency and Responsibility report of 2021, 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 case of human rights-related misuse. In a written submission to PEGA, the NSO Group confirmed that it has terminated contracts with EU Member States^{1a}, supposedly breaching the human rights clauses. The NSO Group has not clarified if it has done an examination of the audit logs, and whether the customers in question had consented to such 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 authorities have any evidence. (1118, 1119).

Footnote:

1a. PEGA Committee Hearing with NSO, 21 June 2022;

154 d (new). According to Amnesty International, the transparency report of the NSO Group lacks a proper remediation policy for victims of unlawful surveillance and information on the ongoing lawsuits against the NSO Group is absent^{1a}. As opposed to NSO's Human Rights Policy and HRDD procedure, its spyware continues to be detected on devices of journalists and critics of authoritarian regimes^{1b}. (1120, 1121)

Footnotes:

1a. Amnesty International, NSO Group's new transparency report is 'another missed opportunity', press release, 1 July 2021

1b. NYTimes. U.S. Blacklists Israeli Firm NSO Group Over Spyware.

COMP Paragraph 155

Covered: AM 12 (S&D), AM 1122 (Rapporteur), AM 1123 (Greens),

Fall: AM 16 (S&D)

Export controls

155. Since the Pegasus spyware is qualified as a dual-use technology, it ~~thus~~ needs to receive an export license. The NSO Group companies obtain their export licenses in Israel, Bulgaria and Cyprus²⁹⁷. **The NSO Group itself has confirmed this, but denies the export of the Pegasus spyware from Cyprus and Bulgaria^{297a}. The Cypriot and Bulgarian governments have denied the granting of any export permits to NSO companies in general. Other sources have challenged this, stating that NSO subsidiaries often hide behind a different name in the national business registers. One of NSO's subsidiaries in Cyprus under the name of Circles has however closed its offices in 2020^{297b}. (1122, 1123).** ~~Most of these~~ Licenses are also granted by the Israeli authorities²⁹⁸. Israel is not part of the Wassenaar Arrangement but states that it has incorporated some of its elements in the national Defence Export Control Law 5766,

2007²⁹⁹. The Ministry of Defence's (MOD) Defence Export Control Agency (DECA) is responsible for the issuance of marketing and export licenses³⁰⁰. Following the Pegasus Project revelations and the blacklisting of NSO, the list of eligible countries has been reduced from 102 down to 37, which all need to sign an End Use/User Certificate³⁰¹. In 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.

Footnotes:

297 Amnesty International. *Operating from the shadows. Inside NSO Group's corporate structure*. P. 62.

297 a (new) Amnesty International. *Operating from the shadows. Inside NSO Group's corporate structure*.

297 b (new) VICE. *NSO Group Closes Cyprus Office of Spy Firm*.

298 Amnesty International. *Operating from the shadows. Inside NSO Group's corporate structure*.

299 European Parliamentary Research Service. *Europe's PegasusGate. Countering spyware abuse*.

300 Amnesty International. *Novalpina Capital's reply to NGO coalition letter (15 April 2019) and Citizen Lab letter (06 March 2019)*

301 European Parliamentary Research Service. *Europe's PegasusGate. Countering spyware abuse*

COMP Paragraph 156

Covered: AM 1124 (Rapporteur), AM 1125 (Greens), AM 1126 (Rapporteur), AM 1127 (Greens), AM 1128 (Rapporteur), AM 1129 (Greens), AM 1131 (Rapporteur), AM 1132 (Rapporteur), AM 1133 (Greens), AM 1134 (Rapporteur), AM 1135 (Greens), AM 1136 (Greens), AM 1137 (Rapporteur), AM 1138 (Greens)

Fall: AM 1130 (Greens)

Unethical behaviour triggering lawsuits, blacklisting and investor conflicts

156. In July 2021, a conflict between the three co-founders of Novalpina Capital started to affect the NSO Group's business, eventually leaving the investors to the decision to strip the private equity firm of its control³⁰². 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 their compliance with the US blacklisting. The BRG inquiries of May 2022 were obstructed by the NSO Group's management team³⁰³. A BRG executive stated that cooperation with the NSO Group has become 'virtually non-existent' due to the NSO Group's pressure for continued sales to countries with controversial human rights records³⁰⁴. On 25 April 2022, two of Novalpina former general partners filed a lawsuit at the Luxembourg court against BRG, urging to reinstate Novalpina Capital as general partner and suspending all decisions that have been taken by BRG³⁰⁵. The Luxembourg court has dismissed these demands and BRG remains in charge of the fund controlling the NSO Group³⁰⁶.

Footnotes:

302 *Financial Times*. *Private equity owner of spyware group NSO stripped of control of €1bn fund*.

303 *Financial Times*. *NSO Group keeping owners 'in the dark', manager says*.

304 *The New Yorker*. *How democracies spy on their citizens*.

305 *Letter to Mr Jeroen Lenaers and his Vice Chairs*.

306 *Luxembourg Times*. *Top five stories you may have missed*.

156 a (new). In addition to ownership fall-outs, the US Commerce Department placed the NSO Group on 3 November 2021 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^{1a}. (1124, 1125).

Footnote:

1a. NYTimes. U.S. Blacklists Israeli Firm NSO Group Over Spyware.

156 b (new). In response to the US Blacklisting, Credit Suisse, as one of the creditors of the NSO Group, allegedly pushed the company to continue its sales of the 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 about the pressing for the NSO Group sales^{1a}. (1126, 1127).

Footnote:

1a. Financial Times. Credit Suisse pushed for spyware sales at NSO despite US blacklisting.

156 c (new). A few days after the US blacklisting of NSO, the United States Court of Appeals confirmed the proceeding of Meta’s lawsuit against NSO, immediately followed by a complaint lodged at the federal court by Apple^{1a}. In June 2022, the United States District Court rejected the NSO Group’s claim to immunity in the Apple lawsuit^{1b}. At time of writing, the Apple lawsuit against the NSO Group is still pending. (1128, 1129).

Footnotes:

1a. NYTimes. Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones.

1b. https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/35/

156 d (new). Despite of the US blacklisting, the Biden administration has 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 advice the NSO Group through Francisco Partners. According to the Guardian, he was one of the eight members on NSO’s business ethics committee, allegedly providing him with a vote on the proceedings of proposed NSO sales. Beacon Global Strategies terminated the work with NSO after the pursued sales to Saudi Arabia^{1a}. (1131, 1133)

Footnote:

1a. The Guardian. Biden intelligence advisor previously vetted deals for Israeli NSO Group.

156 e (new). The NSO Group has similarly suffered from departing personnel. Since the murder on Jamal Khashoggi and the growing concerns of the role of Pegasus therein, many employees have left the NSO Group. That same month, co-founder Shalev Hulio stepped down as CEO of the NSO Group and was replaced by Yaron Shohat^{1a}. The NSO group changed policy and now focuses only on NATO members^{1b}. (1132, 1135). In March 2023, it was reported that NSO’s shares were transferred to co-founder Omri Lavie’s investment firm Dufresne Holding^{1c}.

Footnotes:

1a 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?

1b The Guardian. CEO of Israeli Pegasus spyware firm NSO to step down.

1c The Guardian. NSO Group co-founder emerges as new majority owner

156 f (new). *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 as the now controversial Pegasus spyware, considering also the Predator spyware from Intellexa company^{1a}.*

Footnotes:

1a. <https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9>

156 g (new). *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^{1a}. The cooperation between Kurz and Hulio constitutes an indirect but alarming connection between the spyware industry and Peter Thiel and his firm Palantir. (1134, 1136).*

Footnote:

1a OCCRP. Former Austrian Chancellor and ex-NSO Chief Start Cybersecurity Firm; The Times. Former NSO CEO and ex-Austrian Chancellor found startup.

156 h (new). *Dream Security raised \$20 million from several investors, like Adi Shalev who was also involved in NSO investments. Other investors include Yevgeny Dibrov^{1a}, who represents ‘the New Russian voice in what he calls ‘the Russian-Israeli tech ecosystem’^{1b}. (1137, 1138). It shows that, despite the turbulence and economic challenges of the NSO Group, the same names keep on launching new spyware companies within and beyond the EU.*

Footnotes:

1b The Times. Former NSO CEO and ex-Austrian Chancellor found startup.

1c Calcalist. From Russia, With Coding Skills.

COMP Paragraph 157

Covered: AM 1139 (Greens), AM 1140 (Rapporteur), AM 1141 (Rapporteur), AM 1142 (Greens)

Fall:

Black Cube

157. Black Cube is an Israeli private intelligence agency comprised of former employees of Mossad, the Israeli military and Israeli intelligence services³⁰⁷. Their own company website dubs them as a ‘creative intelligence service’ finding ‘tailored solutions to complex business and litigation challenges’³⁰⁸. Black Cube have been involved in a number of public hacking controversies including in the US and Romania³⁰⁹. More particularly, the heads of Black Cube admitted spying on the former chief prosecutor of Romania’s National Anti-Corruption Directorate Laura Kövesi³¹⁰. Kövesi is currently the first European Chief Prosecutor to head the European Public Prosecutor Office (EPPO). Daniel Dragomir - a former Romanian secret agent - was allegedly the person who commissioned Black Cube for the job³¹¹.

Footnotes:

307 The New Yorker, <https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators>, 7 October 2019.

308 <https://www.blackcube.com/>

309 *The New Yorker*, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

310 *Balkan Insight*. *Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case*.

311 *Haaretz*. *Black Cube CEO Suspected of Running Crime Organisation. Revealed: The Romania Interrogation*.

157 a (new). *Critically, it has also been uncovered that they are 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 at in at least one situation in Cyprus. (1139, 1140).*

157 b (new). *Black Cube got involved in Hungary during the 2018 elections, during which time they spied upon various NGOs and persons who had any connection to George Soros and reported back to Orban in order for him to spin their actives in a smear campaign^{1a}. The resulting information from the surveillance of those individuals and NGOs appeared not only in the Hungarian state-controlled media, but also in the Jerusalem Post^{1b}. (1141, 1142).*

Footnotes:

1a Politico, <https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/> 6 July 2018.

1b Politico, <https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/> 6 July 2018.

COMP Paragraph 158

Covered: AM 1143 (Rapporteur), AM 1144 (Rapporteur), AM 1145 (Greens), AM 1146 (Greens),

Fall:

Intellexa Alliance

158. Intellexa was set up in 2019 in Cyprus by Tal Dilian. Dilian served different leadership positions in the Israeli Defence Force before he started a career as ‘intelligence expert, community builder and serial entrepreneur’³¹². On its website, Intellexa Alliance is described as an ‘EU based and regulated company with the purpose to develop and integrate technologies to empower intelligence agencies. Several surveillance vendors that are part of the marketing label of Intellexa Alliance include:

- Cytrox, WiSpear (later renamed under Passitora Ltd)
- Nexa technologies (run by former Amesys managers)
- Poltrex

Footnote:

312. Tal Dilian. *About*.

158 a (new). *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 additionally extract data from Wi-Fi networks. The different vendors under Dilian’s alliance thus allow for a broad assortment of software and services that Intellexa can offer and combine to its clients within and outside of the EU^{1a}. (1143, 1145)*

Footnote:

1a. Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.*

158 b (new). *Parent company of Intellexa Alliance - Thalestris Limited - has different subsidiaries that have corporate presence throughout Ireland, Greece, the British Virgin Islands, Switzerland and Cyprus. Sara Aleksandra Hamou, reportedly the second ex-wife of Tal Dilian, has been the director of Thalestris Limited, and managing director of a subsidiary based in Greece^{1a}. Hamou, originally born in Poland, holds a Cypriot passport issued by the Embassy of Poland in Cyprus^{1b}. (1144, 1146)*

Footnotes:

1a Thalestris Limited. *Annual Report and Consolidated Financial Statements for the period from 28 November 2019 to 31 December 2020.*

1b ReportersUnited. *The Great Nephew and Big Brother.*

COMP Paragraph 159 - 160

Covered: AM 1147 (Rapporteur), AM 1148 (Greens), AM 1149 (Rapporteur), AM 1150 (Greens), AM 1151 (Rapporteur), AM 1152 (Greens), AM 1153 (Greens)

Fall: AM 1154 (Greens),

WiSpear and Cytrox

159. In 2013, Tal Dilian started a Cypriot registered company under the name of Aveledo Ltd., later to be known as Ws WiSpear Systems Ltd. and after that Passitora Ltd³¹³. Stationed in Limassol Cyprus, Wispear mostly sells equipment and software to locate and track individuals through their mobile phone. In an interview to Forbes magazine, Dilian explained the capabilities of the WiSpear software by showing his 9 million dollar worth black van, capable of hacking devices within a range of 500 meters. Additionally, WiSpear owns equipment capable of intercepting data from Wi-Fi networks³¹⁴. Public scandals relating to these products triggered the move of Intellexa's main business activities from Cyprus to Greece.

Footnotes:

313 Open Corporates. *Passitora Ltd.* <https://opencorporates.com/companies/cy/HE318328>

314 Haaretz. *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*

159 a (new). *In 2017, Cytrox Holdings Zrt. was founded in North Macedonia by Ivo Malinkovski. However, the cradle of Cytrox was actually in Tel Aviv, and Malinkovski was just the front man. After the Pegasus Project revelations, Malinkovski tried to erase all traces connecting him to Cytrox. (1147, 1148)*

159 b (new). *Cytrox was the developer of the Predator spyware. In contrast to Pegasus spyware, Predator requires the target to click on a link to install the software^{1a}. When Cytrox was on the verge of bankruptcy, Tal Dilian rescued it with the acquisition costing under 5 million dollars^{1b}. Cytrox was subsequently merged with Dilian's WiSpear^{1c}. This acquisition added the Predator spyware to the arsenal of Intellexa technologies. (1149, 1150). As reported by Lighthouse Reports, in collaboration with Haaretz and Inside Story, Intellexa has secretly and illegally delivered the Predator spyware to the Sudanese Rapid Support Force militia by a Cessna private jet^{1d}.*

Footnotes:

1a European Parliament. *Greece's Predatorgate. The latest chapter in Europe's spyware scandal?*

1b BalkanInsight. *Wine, Weapons and Whatsapp: A Skopje Spyware Scandal.*

1c Pitchbook. *Cytrox overview.*

Id. <https://www.lighthousereports.nl/investigation/flight-of-the-predator/>

159 c (new). According to CitizenLab, several Cytrox companies have been registered in Israel - Cytrox EMEA ltd. and Cytrox Software Ltd. - and in Hungary as Cytrox Holdings Zrt.^{1a} All of the shares of Cytrox Holdings Zrt. and Cytrox EMEA ltd - later renamed to Balinese Ltd. - were transferred to Aliada Group Inc. as registered in the British Virgin Islands. Aliada Group is also the owner of WiSpear. The main shareholders of Aliada Group are Dilian himself, as well as Oz Liv, Meir Shamir and Avi Rubinstein. In December 2020, Rubinstein lodged a complaint against his co-shareholders of Aliada Group 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^{1b}. (1151, 1152).

Footnotes:

1a Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.

1b Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.

159 d (new). On 16 December 2021, CitizenLab released a report stating likely Predator customers were found in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia^{1a}. (1153).

Footnote:

1a CitizenLab: 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/>

Amesys and Nexa Technologies

160. Amesys and Nexa Technologies are also part of Intellexa Alliance, and not free from controversy, as mentioned in the Chapter on France.

COMP Paragraph 161

Covered: AM 1156 (Rapporteur), AM 1157 (Rapporteur), AM 1158 (Greens),

Fall:

Poltrex

161. Poltrex was launched in October 2018 and the sole shareholder of the company was Intellexa ltd as registered in the British Virgin Islands. Israeli Shahak Avni - founder of the Cypriot NCIS Intelligence Services ltd³¹⁵ and 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 the name of Poltrex was changed to Alchemycorp Ltd. Notwithstanding the renaming of Poltrex, the company was still hosted in the Novel Tower - the same location as the address of WiSpear³¹⁶.

Footnotes:

315 Philenews. ΦΑΚΕΛΟΣ: Η Πολιτεία υπέθαλπε Άβνι και Ντίλιαν (1156)

316 CyprusMail. Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.

161 a (new). *When the investigations surrounding Dilian's spyware van were proceeding, the ownership of Alchemycorp Ltd. was transferred to Yaron Levgoren. Levgoren was an employee of Cytrox Holdings^{1a}. According to his LinkedIn he currently represents the Intellexa company Apollo Technologies, based in Greece^{1b}. (1157, 1158)*

Footnotes:

1a. Philenews. How the spyware scandal in Greece is related to Cyprus.

1b. <https://ca.linkedin.com/in/yaron-levgoren-116948101>

COMP Paragraph -162 a (new) to Paragraph -162 k (new)

Covered: AM 1159 (Rapporteur), AM 1160 (Rapporteur), AM 1161 (Rapporteur), AM 1162 (Rapporteur), AM 1163 (Rapporteur), AM 1164 (Rapporteur), AM 1165 (Rapporteur), AM 1166 (Rapporteur)

Fall:

Verint/Cognyte (1159)

-162 a (new). *Verint is an Israeli-American cyber company that has many subsidiaries all over the world. In Europe alone, Verint is registered as of 2021 in Bulgaria, the Netherlands, Cyprus, Germany and France. Verint also had subsidiaries operating under the name Cognyte. These subsidiaries operate independently since 2021 when Verint concluded the spin-off of its intelligence and cyber activities to Cognyte^{1a}. 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 Informationssysteme b.h. OHG) and Romania (Cognyte Romania S.R.L.)^{1b}. (1160)*

Footnotes:

1a Calcalistech. Verint completes spin-off of its defense activities into new company Cognyte Software.

1b <https://www.sec.gov/Archives/edgar/data/1824814/000182481421000007/exhibit81.htm>

-162 b (new). *Verint has sold surveillance tools to several repressive governments, amongst others in Azerbaijan, Indonesia and in South Sudan. In the case of the latter, the 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 enabled the NSS to listen in on all Sudanese telecommunications^{1a}. 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. According to Verint, the division with Cognyte was already in place for many years before the official spin-off in 2021, distancing themselves from the alleged export of surveillance equipment to countries with poor human rights records^{1b}. (1161)*

Footnotes:

1a Haaretz. Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds; Amnesty International. South Sudan: Rampant abusive surveillance by NSS instils climate of fear.

1b Haaretz. Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds;

-162 c (new). *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^{1a}. Cognyte subsidiary UTX Technologies, registered in Cyprus, reportedly also received licenses for the export of monitoring software to Mexico, United Arab Emirates, Nigeria, Israel, Peru, Colombia,*

Brazil, South Korea and Thailand between September 2014 and March 2015^{1b}. Four of these countries overlap with Cognyte customers identified in the 2021 Meta report. In addition, UTX Technologies secured an agreement with Bangladesh for a Web Intelligence System for 2 million dollars in 2019 and for a cellular tracking system for 500.000 dollar in 2021^{1c}. (1162)

Footnotes:

1a Meta. Threat Report on the Surveillance-for-Hire Industry.

1b Philenews. Cyprus is a pioneer in software exports (documents).

1c Haaretz. Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Records.

-162 d (new). On January 15 2023, media reported that Israel's Cognyte Software Ltd won a tender for the sale of its interception spyware to Myanmar, one month prior to the military coup that took place in February 2021. The purchase of Cognyte's spyware by Myanmar was officially placed on 30 December 2020^{1a}. (1163)

Footnote:

1a Reuters. Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup- documents.

-162 e (new). Next to the export to third countries, Cognyte has also facilitated the transport of tracking equipment to Member States. Through UTX Technologies, registered in Cyprus, Gi2 technology was shipped to another Cognyte subsidiary in Germany under the name of Syborg Informationsysteme^{1a}. This Gi2 technology was reportedly also sent to a Verint subsidiary in Poland "for demonstrations 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^{1b}. These shipments took place between 2013 and 2014. At that time Verint and Cognyte were still part of the same company structure. (1164)

Footnotes:

1a <https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex81.htm>

1b Philenews. Cyprus is a pioneer in software exports (documents)

-162 f (new). UTX Technologies also sold monitoring systems in 2013 to a French export company under the name of COFREXPORT^{1a}. This company has ceased operations and is closed at time of writing. (1165)

Footnote:

1a Philenews. Cyprus is a pioneer in software exports (documents)

-162 g (new). Like many other spyware vendors, Cognyte's company structure is highly complex, due to name changes, divisions and spin-offs overtime. The Cognyte subsidiaries show however that EU Member States are not only used to export surveillance equipment from, but also function as a foothold to sell and ship surveillance equipment within Europe. Israeli spyware companies thus benefit from the EU's internal market, facilitating the transport of their equipment to both their own subsidiaries as well as to new companies registered in EU Member States. (1166).

QuaDream

-162 h (new). 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 product 'Reign', a spyware product that allegedly makes use of zero-click exploits and consists of a self-destructing feature that

erases the traces of infection. This type of spyware holds different functionalities like recording audio, tracking locations, searching for files, and taking pictures through both cameras.^{1a}

-162 i (new). According to CitizenLab and a Microsoft Threat Intelligence analysis, QuaDream systems are operating from Bulgaria, Czech Republic, Hungary, Romania, Ghana, Israel, Mexico, Singapore, the United Arab Emirates and Uzbekistan. In addition, the findings identified at least 5 civil society victims that are located in North America, Central Asia, Southeast Asia, Europe and the Middle East.^{1b}

-162 j (new). In 2017, a company under the name InReach was registered in Cyprus. This company was solely founded for the promotion of QuaDream products, like Reign, outside of Israel. Reportedly, QuaDream used InReach to sell its products to customers to circumvent Israeli export controls. Many of the key employees of both companies have worked for the NSO Group, Verint and UT-X Technologies.^{1c}

-162 k (new). Following the reporting of CitizenLab and the Microsoft Threat Intelligence analysis, it was announced on 16 April 2023 that QuaDream halted its operations in Israel. According to Haaretz, the company was already struggling with declining sales and leaving employees in the preceding months^{1d}.

Footnotes:

1a. <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?hs=1681386702066>

1b. <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/>;

1c. <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?hs=1681386702066>

1d. <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-adeb-ebdc048c0000>

COMP Paragraph 162

Covered: AM 1167 (Rapporteur), AM 1168 (Greens), AM 1169 (Rapporteur), AM 1170 (Greens), AM 1171 (Rapporteur), AM 1172 (Greens)

Fall:

Candiru

162. Candiru is another Israeli registered firm producing spyware products. The company was founded in 2014 by Ya'acov Weitzman and Eran Shorer. Both founders have a history in the IDF Military Intelligence Unit 8200 and both were former employees of the NSO Group³¹⁷. Former investor in the NSO Group Isaac Zack became the largest shareholder of Candiru. The company sells spyware for the hacking of computers and servers³¹⁸. Disclosed information of a project proposal highlights that Candiru sells its equipment per number of simultaneous

infections. That is, the number of targets that can be targeted with the spyware at one moment in time. For example, for 16 million dollars, a customer receives an unlimited number of spyware attempts, but can only target 10 devices concomitantly. A customer can purchase 15 additional devices for an extra 1.5 million dollar³¹⁹.

Footnotes:

317 Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers

318 Haaretz. Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.

319 CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.

162 a (new). According to a TheMarker inquiry, Candiru now also offers spyware to break into mobile devices^{1a}. It solely sells its spyware to governments and its clientele consists of "Europe, the former Soviet Union, the Persian Gulf, Asia and Latin America"^{1b}. As highlighted in the chapter on Spain, four people out of the 65 victims were targeted with Candiru, and at least two people were targeted with both Candiru and Pegasus^{1c}. (1167, 1168).

Footnotes

1a Haaretz. Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.

1b CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.

1c CitizenLab. CatalanGate. Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru.

162 b (new). As with the other spyware vendors, corporate obfuscation lays at the heart of this company, as it has undergone several name changes throughout the last couple of years. The company has changed its names to DF Associates Ltd. in 2017, Grindavik Solutions Ltd in 2018, Taveta Ltd in 2019 and the most recent change to Saito Tech Ltd in 2020^{1a}. For sake of clarity, we will refer to the company as Candiru. (1169, 1170).

Footnote:

1a CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.

162 c (new). Just like the NSO Group, Candiru was similarly 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 CEO of the NSO Group Shalev Hulio allegedly was 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^{1a}. ~~At a later stage Hulio and Candiru became rivals, as Hulio heard from Francisco Partners that Candiru wanted to compete with NSO Group^{1b}.~~ On July 1 2022, security researchers identified a novel Chrome zero-day exploit that was used by Candiru to target individuals in Lebanon, Palestine, Yemen and Turkey^{1c}. The exploit was addressed by Google and has since also been patched by Microsoft and Apple^{1d}. (1171, 1172).

Footnotes:

1a Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers

1b Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers

1c TechCrunch. Spyware maker Candiru linked to Chrome zero-day targeting journalists.

1d The HackerNews. Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists.

COMP Paragraph 163

Covered: AM 1173 (Rapporteur), AM 1174 (Greens), AM 1175 (Rapporteur), AM 1176 (Greens)

Fall:

Tykelab and RCS Lab

163. In August 2022, Lighthouse Report reported that Tykelab, a company based in Rome and belonging to the RCS lab, has been using dozens of phone networks, often on 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 left on the devices³²⁰. In over just two days in June 2022, the company probed networks in almost every country in the world³²¹. On its website, Tykelab ‘combines twenty years of experience in the design, implementation and maintenance of Core Network Telco solutions, a strong expertise in delivering Managed Services, Customer-based System Integration and Mobile App developments.’³²²

Footnotes:

320 <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

321 <https://euobserver.com/digital/155849>

322 <http://www.tykelab.it/wp/about/>

163 a (new). Lighthouse Report’s investigation also highlighted the role of the telecom industry, where the leasing of phone network access points or “global titles” allows for 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^{1a}. (1173, 1174).

Footnote:

1a <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

163 b (new). Tykelab is a part of RCS Lab, an Italian company known for its interception activities in Italy and abroad, which was brought to light by an announcement of a third company, Cy4Gate, which acquired RCS Lab. RCS Lab has off-shoots in France, Germany and Spain^{1a}. RCS Lab has another concealed subsidiary, Azienda Informatica Italiana, which builds interception software for Android and iPhone devices^{1b}. (1175, 1176).

Footnotes:

1a <https://euobserver.com/digital/155849>

1b <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

COMP Paragraph 164

Covered: AM 1177 (Rapporteur), AM 1178 (Greens), AM 1179 (Rapporteur), AM 1180 (Greens), AM 1181 (Greens)

Fall:

Hermit spyware

164. RCS Lab has developed Hermit, spyware that can be used to remotely activate the phone’s microphone, as well as record calls, access messages, call logs, contacts, and photos³²³. 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 providers to disable the target’s mobile data connectivity. Once 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 the reason why most of the applications masqueraded as mobile carrier applications. When ISP involvement is not possible, applications are masqueraded as messaging applications. Victims targeted with RCS Lab's spyware were located in Italy and Kazakhstan³²⁴, and it was also found in Romania³²⁵.

Footnotes

323 <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

324 <https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/>

325 <https://www.lighthousereports.nl/investigation/revealing-europes-nso>

164 a (new). *A Threat Intelligence Researcher of cyber security firm Lookout, Justin Albrecht, said that although Hermit's method of installation was less sophisticated than that of Pegasus, its capabilities were similar. Hermit needs a phone user to click on an infected link for it to compromise a device^{1a}. (1177, 1178).*

Footnote:

1a <https://euobserver.com/digital/155849>

164 b (new). *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."^{1a} However, it is not possible to verify if Cy4gate Group, including RCS Lab, adheres to its own declared standards. (1179, 1180).*

Footnote:

1a <https://euobserver.com/digital/155849>

164 c (new). *According to an investigation from Lighthouse Reports 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^{1a}.(1181).*

Footnote

1a Lighthouse Reports: Revealing Europe's NSO. <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

COMP Paragraph 165

Covered: AM 1182 (Rapporteur), AM 1183 (Greens), AM 1184 (Greens), AM 1185 (Rapporteur), AM 1186 (Greens), AM 1187 (Rapporteur)

Fall:

DSIRF - Decision Supporting Information Research and Forensic

165. A company that has recently become subject of criminal proceedings by the Austrian Ministry of Justice is DSIRF GmbH (LLC)³²⁶, an Austrian company based in Vienna with a parent company in Liechtenstein that was founded in 2016, which 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.'³²⁷ DSIRF evidently sells to non-state actors.

Footnotes:

326 DSIRF is an abbreviation for "Decision Supporting Information Research and Forensic"

327 <https://dsirf.eu/about/>

165 a (new). *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"^{1a}. In 2020 DSIRF valued its software Subzero with 245 million euros. (1182, 1183)*

Footnote:

1a <https://netzpolitik.org/2021/dsirf-wir-enthuelen-den-staatstrojaner-subzero-aus-oesterreich/>

165 b (new). *The connection with Russia becomes clear from links of several high level staff members of DSIRF. The owner of DSIRF is Peter Dietenberger, a "man with best connections in the Kremlin" and a "door opener of western companies in Putin's empire"^{1a}. Dietenberger lived several years in Russia, had a Russian company and several Russian business partners. One of his Russian business partners, Boris Vasilyev, was also in the board of directors of DSIRF. DSIRF names 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 is sanctioned by the US since 2018) and Florian Schneider (partner at the large business law firm Dentons in Moscow)^{1b}. "Russian Machines", a company owned by the oligarch Oleg Deripaska, is said to be using the services of DSIRF. The powerful local entrepreneur Siegfried "Sigi" Wolf, who advised former Chancellor Sebastian Kurz on economic issues, is considered a confidante of Deripaska^{1c}. Also Jan Marsalek, an alleged criminal wanted on an Interpol arrest warrant for commercial fraud charges amounting to billions, among other financial and economic offenses, is involved. In August 2018, he received an email from Florian Stermann (Secretary General of the Russian-Austrian Friendship Society, and considered in investigations by the public prosecutor's office to be a "confidant" of the FPÖ)^{1d} with a company presentation of DSIRF. Already in 2013, he allegedly tried to sell spyware of the Italian company Hacking Team to Grenada. He is said to hide in Moscow at the moment, under the care of the FSB, the Russian secret service^{1e}. (1184, 1185).*

Footnotes:

1a 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

1b <https://netzpolitik.org/2021/dsirf-wir-enthuelen-den-staatstrojaner-subzero-aus-oesterreich/>

1c <https://www.derstandard.at/story/2000131301583/causa-marsalek-die-verbindungen-einer-spionagefirma-werfen-fragen-auf>

1d https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spyonage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
1e <https://netzpolitik.org/2021/dsirr-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/>;
<https://www.dw.com/en/wanted-wirecard-executive-jan-marsalak-reportedly-hiding-in-moscow/a-61440213>

165 c (new). *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^{1a}. Austria currently has no legal basis for the unauthorised deployment of spyware like Subzero by public authorities, and it is also illegal if one private company would 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 regards to Dual Use Goods^{1b}. On 7 October 2022, the Austrian Federal Ministry of Labour and Economic Affairs stated that it had not issued an export license to DSIRF^{1c}, and according to the Austrian Federal Ministry for Justice Affairs, the Vienna Public Prosecutor's Office has started a criminal investigation into DSIRF^{1d}. The use of the Subzero spyware against targets in Austria means that either a private or public authority in Austria has applied the software illegally, the software was used by a foreign actor and export restrictions were violated by DSIRF or the software was exported to another Member State and used from there legally or illegally against an Austrian target. The investigation is still ongoing. (1186, 1187).*

Footnotes:

1a <https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/>

1b <https://en.epicenter.works/document/4236>

1c 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 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml

1d 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

COMP Paragraph 166

Covered: AM 1188 (Rapporteur), AM 1189 (Greens),

Fall:

FinFisher

166. Important to mention in this report is the criminal investigation into and bankruptcy of FinFisher, a former spyware company based in Munich, Germany. FinFisher is a network of companies, founded in 2008, originally with strong ties to the British network of companies under the brand 'Gamma'. FinFisher promoted its spyware as 'complete IT intrusion portfolio', with its software being used by dozens of countries all over the world³²⁸, including 11 EU Member States³²⁹ and 13 'not-free' countries³³⁰.

Footnotes:

328 <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/> -

<https://wikileaks.org/spyfiles4/customers.html>

329 Belgium, Czech Republic, Estonia, Germany, Hungary, Italy, Netherlands, Romania, Slovakia, Slovenia, Spain

330 Angola, Bahrain, Bangladesh, Egypt, Ethiopia, Gabon, Jordan, Kazakhstan, Myanmar, Oman, Qatar, Saudi Arabia, Turkey

166 a (new). *In 2017, Finfisher's product FinSpy appeared in Turkey on a fake version of a mobilization website for the Turkish opposition. The software was disguised as a downloadable app recommended to participants in anti-government demonstrations^{1a}. Finfisher itself advertised its products as solely fighting crime. In 2019, a criminal complaint was filed against Finfisher by Gesellschaft für Freiheitsrechte (GFF), Reporter ohne Grenzen (RSF Germany), the blog netzpolitik.org and the European Center for Constitutional and Human Rights (ECCHR), for exporting its spyware without the necessary export license from the German Federal Office for Economic Affairs and Export Control. It thereby violated the EU Dual-Use Regulation and corresponding German national law. Following the complaint, the Public Prosecutor's Office of Munich investigated FinFisher, and in October 2020 it searched 15 business premises of the FinFisher group of companies in Germany and Romania and private residences. In 2021, the Munich District Court approved the seizure by the Public Prosecutor's Office's of Finfisher's bank accounts, in order to ensure confiscation of illegally obtained profits after FinFisher's possible 'conviction. However, FinFisher declared insolvency in February 2022. Business operations have ceased, the office has been closed, and all 22 employees were dismissed^{1b}. The criminal investigations into the people responsible for FinFisher's activities are still ongoing. (1188, 1189)*

Footnotes:

1a <https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/>

1b <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

Compromises on the European Union's capacity to respond

III. The European Union's capacity to respond

COMP Paragraph 167

Covered: 1193 (EPP), 1195 (rapporteur), 1196 (The Left),
Fall: 1191 (ID), 1192 (ECR), 1194 (NI), 1197 (Hristov), 1248 (EPP)

167. 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 **fundamental rights of individual citizens' rights.** **The EU has few powers to act on these threats, but it turns out to be ill-equipped against potential criminal activity by national authorities, even if it affects the EU.** ~~The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game. Under the Treaties national security remains the exclusive competence of the Member~~

States, *but it must still comply with the fundamental rights and democratic norms embedded in EU law* define national security unilaterally, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness. *Also political factors limit the EU's power to act.* The European Commission, as guardian of the EU treaties, has *not maximised its efforts in enforcing EU law, by using all legally possible instruments.* grown reticent when it comes to enforcing EU law³³¹. This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers *very narrowly in the narrowest possible way, as concerning almost exclusively the correct transposition of EU law into national law. The Commission considers that addressing transgressions of EU law are 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.* The EU turns out to be quite powerless against potential criminal activity by national authorities, even if it affects the EU. and respect for the exclusive national competences risks turning in to impunity. 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.

Footnote:

~~331~~ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

COMP Paragraph 168

Covered: 1198 (rapporteur),

Fall: 1199 (ID), 1200 (ECR), 1201 (EPP), 1202 (NI), 1203 (EPP), 1204 (NI), 1205 (Hristov), 1206 (EPP)

European Commission

168. *Following press reports about the use of spyware in Member States and questions by PEGA*, the European Commission, in its response to the spyware scandal, has ~~so far~~ *initially limited itself to writing only written* letters requesting clarification from the governments of Poland, Hungary, Spain, ~~and~~ Greece, *Cyprus and France*. However, it would seem that this ~~timid~~ admonition by the Commission ~~will~~ *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 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.

168 a (new). *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’^{1a}. The Commission asked specific questions about i.a. the purpose of use of spyware, the authorities authorised to deploy it, on the national definition of national security, relevant legislation that governs the processing of data for national security purposes, safeguards, prior authorisation by a court of independent administrative authority, oversight and notification, with a deadline of 31 January 2023 to respond. On 28 March 2023, Commissioner Reynders stated in PEGA that a large majority of the Member States had replied, but that it is still in the process of collecting the Member State responses to this mapping exercise, and that it would ‘carefully assess’ these replies. Based on this mapping exercise, the Commission will reflect on its options regarding the use of spyware in Member States. No specific end date for the assessment of the Commission is foreseen however, ‘given the evolving and sensitive nature of the assessment’. The Commission also mentioned that it will follow very closely the findings of PEGA.*

Footnote:

1a Letter DG JUST to Member States. Ref. Ares(2022)8885417, 21 December 2022.

COMP Paragraph 169 to 170 a (new)

Covered: 1207, new text (rapporteur), 1208 (EPP)

Fall:

169. Unlike the US, *which has responded to the revelations with blacklisting companies, carrying out investigations, including on EU territory, and with 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*~~European market~~. 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.*

Covered: 1210 (rapporteur)

Fall: 1209 (EPP), 1211 (Hristov), 1212 (ID), 1213 (ECR)

170. 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), there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission *as Guardian of the Treaties* is ~~weak~~ **not performed to its full potential**. It tends to limit itself to verifying if a Member State has correctly transposed EU laws in national laws. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report³³² of 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. ~~Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors.~~ **The implementation of the ePrivacy Directive and case law deriving from it is poor. The Commission refers to the Member States as responsible for implementation and enforcement, but it does not take action when Member States fail to do so.** Without proper and meaningful enforcement, EU laws are mere paper tigers ~~that~~ **become ineffective and** create ample space for the illegitimate use of spyware.

Footnote:

332

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223>

Covered: 1214 (EPP)

Fall:

170 a (new). *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 laws, 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 subject's rights. The European Commission should urgently assess the implementation in all Member States and identify the most serious shortcomings. The Commission should develop concrete guidance to Member States on implementation in order to ensure that EU standards are respected across the Union. Furthermore, where necessary, the Commission should start infringement procedures in cases the Directive was not transposed correctly and there is lack of willingness from a Member States to correct it.*

COMP Paragraph 171 - 171 a (new)

Covered: 1218 (rapporteur),

Fall: 1217 (ECR), AMs 1215 (EPP), 1216 (ID), 1219 (Hristov)

European Parliament

171. The European Parliament has set up the PEGA inquiry committee, 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 ~~eynical~~ **disturbing** that the European Parliament does not have

the full powers to investigate, when some of its own members ~~are victims of illegal surveillance~~ *have been targeted with spyware*.

COMP Paragraph 172

Covered: AM 1224 (rapporteur):

Fall: AMs 1220 (ECR), 1221, 1222, 1223 (identical; ID, ECR, EPP).

European Council and Council of Ministers

172. Although the 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 Parliament³. In doing so, they have fully acknowledged that it is in fact a matter for the Council. ~~However, responsibility is not a menu that you can pick and choose from: you cannot only selectively deal with procedural matters, but not the substance.~~

COMP Paragraph 173

Covered: 1228 (rapporteur)

Fall: 1225 (ECR), 1226 (ID), 1227 (EPP), 1229 (NI)

173. 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. ~~The omertà and lack of cooperation of the Council does not bode well for any future regulatory initiatives. The Council is a legislator, but it may well be reluctant to regulate its own members.~~

No CA on para 174. Vote on AMs 1230 (ECR), 1231 (EPP), 1232 (NI), 1233 (EPP). Voting recommendation: AGAINST

COMP Paragraph 175 to Paragraph 177

Europol

Covers: 1234 (EPP)

~~175. Europol was requested to assist the Cypriot police and an academic expert in conducting a three-level forensic examination of the equipment found in the black van of Tal Dilian in 2019. During the PEGA hearing on 30 August 2022, Europol made no reference to~~

³ Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

~~this, despite questions by Members on Europol's role in investigating spyware in the EU. It has not been mentioned since.~~

Covered: 1236 (EPP), 1240 (rapporteur), 1241 (EPP), 1243 (The Left)

Fall: 1235 (The Left), 1237 (ECR), 1238, 1239 (ID), 1242 (ECR)

176-177. 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 Art 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. ~~This problem is made worse when the Member State authorities are themselves complicit in the crimes.~~ 177. However, Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State³³⁴, but so far it has ~~been reluctant to make~~ **not made** use of those powers. ~~Europol wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas.~~

Footnote:

334 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.

COMP Paragraph 178

Covered: 1245 (rapporteur)

Fall: 1244 (ECR), 1246 (NI), 1247 (EPP)

178. On 28 September 2022, PEGA wrote a letter to Europol³³⁵, urging it to make use of its new powers under Article 6 of the Europol Regulation³³⁶. In a letter of reply dated 13 October 2022³³⁷, Europol stated that it has '*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 were sent to Greece, Hungary, Bulgaria, Spain and Poland. One of the five Member States has meanwhile confirmed to Europol. Following the response by the five Member States to Europol's letter, Europol mentioned that none of them would have "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 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 has 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 ~~which countries the letter refers to, nor~~ 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* ~~inquiry by one Member State~~ concerns the abuse of spyware by EU Member State governments or by third countries.

Footnotes:

335 https://twitter.com/EP_PegaInquiry/status/1576855144574377984

336 "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."

337 File no 1260379.

COMP Paragraph 180

Covered: new text (rapporteur)

Fall: 1249 (EPP), 1250 (ECR)

180. 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'³³⁸. **Moreover, in March 2023 US President Biden issued an Executive Order largely 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.**

Footnote:

338 <https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ>

AMs 1251, 1253-1263 (Greens): out of place. Insert in chapters on Third countries/external relations, and research. Voting recommendation: IN FAVOUR

No CA on para 181. Vote on AM 1264 (ECR). Voting recommendation: AGAINST

COMP Paragraph 181 a (new)

Covered: 1252 (Greens), 1265 (rapporteur)

Fall: 1266 (rapporteur)

(New) Ombudsman

181 a (new) On 28 November 2022, the EU Ombudsman concluded that the European Commission 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 (EUTF). The conclusions followed from a complaint by several civil society organisations. In Niger, the Fund allocated €11.5 million for supply with surveillance equipment, including surveillance software, a wiretapping centre, and an international mobile subscriber identity (IMSI) catcher^{1a}, despite repression against activists in the country. To address the identified shortcomings she identified, the Ombudsman recommended made a suggestion for improvement to ensure that for future EU Trust Fund projects, there is a prior human rights impact assessment to take place.

Footnote:

1a https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf

COMP Paragraph 182

Covered: 1268 (EPP)

Other EU bodies

182. The European Data Protection Board, the European Data Protection Supervisor, ~~the EU Ombudsman~~, 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, ~~and in covering them up. Additionally, t.~~ 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.

No CA on para 182a (new). Vote on AMs 1267, 1270, 1271 (EPP), 1269 (Greens). Voting recommendation: AGAINST

AMs 1272-1281 (Greens) Voted together: voting recommendation of rapporteur: AGAINST.

Citations: Voted together. Voting recommendation of rapporteur: AGAINST