



**2022/2077(INI)**

28.11.2022

## **DRAFT REPORT**

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

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

Rapporteur: Sophie in 't Veld

**CONTENTS**

	<b>Page</b>
DRAFT RESULTS.....	3
EXPLANATORY STATEMENT.....	51

## DRAFT RESULTS

### **of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI))<sup>1</sup>**

*The European Parliament,*

- having regard to Article 226 of the Treaty on the Functioning of the European Union (TFEU),
- having regard to its decision of 10 March 2022 setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee,
- having regard to the report of the committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware (A9-0000/2022).

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

*I.A 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 of 2016, Former Prime Minister and current MEP Beata Szydło, and former Foreign Minister Witold Waszczykowski, attended dinner at the home of then

---

<sup>1</sup> The draft report is based on the document where the rapporteur set her findings. Any person named in the course of the inquiry to whom this might prove prejudicial shall have the right to be heard by the Committee. The Secretariat may be reached at [pega-secretariat@europarl.europa.eu](mailto:pega-secretariat@europarl.europa.eu).

Israeli Prime Minister Benjamin Netanyahu<sup>2</sup>. The following year in July, Szydło and Netanyahu met with the heads of governments of the Visegrad Group countries. They allegedly discussed ‘strengthening cooperation in the area of innovation and high technologies’ and ‘issues related to the broadly understood security of citizens’<sup>3</sup>. Not long after this meeting took place in 2017, Pegasus was acquired by the Polish government following a meeting between Prime Minister Mateusz Morawiecki, Hungarian Prime Minister Viktor Orbán and Netanyahu<sup>4</sup>. Despite initial denials, in January 2022 PiS leader Jarosław Kaczyński confirmed the purchase of spyware by the Polish government<sup>5 6 7</sup>.

## Legal Framework

4. In 2014, the Constitutional Tribunal conducted a review of the Police Act and other existing laws governing surveillance of citizens that were deemed incompatible with the Polish Constitution<sup>8</sup>. The Tribunal concluded by issuing a judgement containing specific recommendations and an 18-month timeline within which legislative changes were to be implemented<sup>9</sup>. Following the 2015 elections, the new government introduced legislative changes. However, the resulting Act of 15 January 2016 Amending the 1990 Police Act and Certain Other Acts (hereinafter the 2016 Police Act) did not rectify any of the gaps in the law, as was required by the Constitutional Court<sup>10</sup>. Instead, the 2016 Police Act has weakened the already lackluster provisions that do not protect the rights of citizens or create proper oversight and compounded the ever-growing distance between the Polish legislature and the rule of law.

## Anti-Terrorism Law 2016

5. In addition to the 2016 Police Act, the Polish government also adopted a law governing the surveillance of foreign citizens in 2016 that it dubs the ‘anti-terrorism law’. The articles of the Act stipulate that non-Polish citizens can be monitored without their consent for a period of three months if their identity is ‘doubtful’, including through wire-tapping of phones, collection of fingerprints, biometric photos and DNA, and the obligation to register pre-paid phone cards<sup>11</sup>. The prosecutor general is responsible for

---

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

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

<sup>4</sup> Financieele Dagblad, ‘De wereld deze week: het beste uit de internationale pers.’ 7 January, 2022.

<sup>5</sup> Financieele Dagblad, ‘Liberalen Europarlement eisen onderzoek naar spionagesoftware’, 12 January 2022.

<sup>6</sup> Politico, <https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/>, 7 January 2022.

<sup>7</sup> Financial Times, <https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e>, 8 February 2022.

<sup>8</sup> 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).

<sup>9</sup> <https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani>

<sup>10</sup> Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

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

ordering the destruction of non-relevant materials and, Zbigniew Ziobro, the PiS Minister of Justice, currently holds that office<sup>12 13</sup>.

## 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, the Act was later rewritten in March 2016 in order to include Article 168a<sup>14</sup>. 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<sup>15</sup>.

## Telecommunications Law of 16 July 2004

7. The law governing telecommunications in Poland includes provisions for the Police to gain access to telecommunication data for free and in certain cases without the participation of employees<sup>16</sup>. This can be done under the vague justification of ‘discovering crimes’. The prosecutor then decides how to proceed on receipt of this data, and indeed is given a significant amount of power in the Act, which is a political decision, given that Ziobro is in that role<sup>17 18</sup>.

## Ex-ante Scrutiny

8. Although surveillance requires judicial authorisation in principle in Poland, in practice the authorisation procedure no longer serves as a safeguard against abuse, but rather as a means to grant a veneer of legality to surveillance 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 services<sup>19</sup>. For the assessment of the application, judges only have the information provided by the applicant (i.e. the special services) at their disposal, and it is the prosecutor who decides what material is relevant to be submitted<sup>20</sup>. The information is often merely a summary, sometimes excluding even the

---

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

<sup>13</sup> EDRI, <https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/>, 29 June 2016.

<sup>14</sup> 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>

<sup>15</sup> <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>

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

<sup>17</sup> Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

<sup>18</sup> Helsinki Foundation for Human Rights, [https://www.hfhr.pl/wp-content/uploads/2016/05/HFHR\\_hand\\_out\\_Venice\\_Commission\\_Act\\_on\\_Police\\_FNL.pdf](https://www.hfhr.pl/wp-content/uploads/2016/05/HFHR_hand_out_Venice_Commission_Act_on_Police_FNL.pdf), 28 April 2016 at pg. 18 [hereinafter HFHR Report].

<sup>19</sup> Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

<sup>20</sup> Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

most basic details regarding the target (name, profession, the crime of which he/she is suspected), and the surveillance methods to be used.

## 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 the Parliamentary Oversight Committee for the Special Services (KSS) was rejected, and the ruling parties installed PiS members Waldemar Andzel as Chairman and Mr. Jarosław Krajewski as Deputy Chairman<sup>21</sup>. The government parties have the absolute majority in the committee<sup>22</sup>. Moreover, the government majority in the Sejm rejected calls for a parliamentary investigation into the allegations of the illegitimate use of spyware<sup>23 24 25 26 27</sup>. The Senate on the other hand, where the government parties hold no majority, did set up an inquiry committee, but the Senate lacks the powers of inquiry of the Sejm<sup>28</sup>.

## Reporting

10. Under the 2016 Police Act, Police are only required to submit semi-annual reports to the courts regarding the number of collections of telecommunication, postal or internet data along with their legal reasoning (relating to the protection of human life or health or supporting search and rescue)<sup>29</sup>. These reports can only be done *ex-post* and are not made public. If there is an issue with the submission, the court will submit their findings in response within 30 days but they cannot order the destruction of any data even if they find incompatibilities with the law. Critically, these supervisory actions are only optional, not mandatory<sup>30</sup>.

## Redress

11. So far, the Polish prosecutor has not launched an inquiry, despite the ample evidence that serious crimes have been committed. It seems that only the case of prosecutor Ewa Wrzosek has been taken up by the courts. Wrzosek initially filed her case with the office of the Prosecutor, however upon their official refusal to take up the case, she was

---

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

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

<sup>23</sup> AP, <https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422> 17 January 2022.

<sup>24</sup> European Commission Rule of Law 2022 Report, Poland Specific Chapter, [https://ec.europa.eu/info/sites/default/files/48\\_1\\_194008\\_coun\\_chap\\_poland\\_en.pdf](https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf) at pg. 27.

<sup>25</sup> AP, <https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab>, 23 December 2021.

<sup>26</sup> The Guardian, ‘Polish senators draft law to regulate spyware after anti-Pegasus testimony’, 24 January 2022.

<sup>27</sup> Politico, <https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/>, 18 January 2022.

<sup>28</sup> European Commission Rule of Law 2022 Report, Poland Specific Chapter, [https://ec.europa.eu/info/sites/default/files/48\\_1\\_194008\\_coun\\_chap\\_poland\\_en.pdf](https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf) at pg. 27, footnote 220.

<sup>29</sup> Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

<sup>30</sup> HFHR Report at pg.4.

able to appeal to the Courts. In late September 2022, the Warsaw District Court (Mokotów) ordered the prosecutor to begin an investigation<sup>31</sup>.

## Public Scrutiny

12. 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 Senator 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.

## Political Control

13. Many key positions in the entire chain are held by members or loyalists of the government parties. Minister of the Interior and Coordinator of the Special Services Kaminski was convicted in 2015 of abuse of power and sentenced to three years imprisonment<sup>32</sup>. But 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 ECJ, 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 co-operate with the European Parliament Pegasus Special Inquiry Committee<sup>33</sup>.

## The Targets

14. Following the investigations of the Associated Press and the Citizen Lab researchers at the University of Toronto, it was revealed that at least three persons had been targeted in Poland in 2019<sup>34</sup>. Those targets were namely opposition Senator Krzysztof Brejza, lawyer Roman Giertych, and prosecutor Ewa Wrzosek, who were hacked with Pegasus spyware that was obtained by the government in 2017<sup>35</sup>. While the government has confirmed the purchase of the software from NSO group, it has not officially acknowledged that any specific persons were targeted. None of the 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 political office.

## Senator Krzysztof Brejza

---

<sup>31</sup> Wyborcza, <https://wyborcza.pl/7,75398,28963729,pegasus-w-telefonie-ewy-wrzosek-prokuratura-odmowila-sad-kaze.html> , 28 September 2022.

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

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

<sup>34</sup> 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.

<sup>35</sup> Financieele Dagblad, 'De wereld deze week: het beste uit de internationale pers.' 7 January, 2022.

15. Senator Krzysztof Brejza was serving as campaign leader of the opposition party Civic Platform when he was the victim of hacking with spyware<sup>36</sup>. There were 33 attacks on Brejza's phone while he was running the Civic Platform campaign in 2019, with the attacks beginning on 26 April 2019 and continuing until 23 October 2019, just days after the end of the election cycle<sup>37</sup>.

### **Roman Giertych**

16. Roman Giertych was targeted with Pegasus spyware during the concluding weeks of the 2019 parliamentary elections. Between September and December of 2019, Giertych was hacked as many as 18 times, the majority of which took place just before the October 13th 2019 election date. At that time, he was serving as the lawyer of opposition leader Donald Tusk. During that period, Giertych was also representing Radek Sikorski, the former Foreign Minister and current MEP with the European People's Party (EPP). Sikorski was 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 conversations<sup>38</sup>.

### **Ewa Wrzosek**

17. Prosecutor Ewa Wrzosek was the victim of hacking with Pegasus spyware as many as 6 times between the 24th of June and the 19th of August 2020<sup>39</sup>. Wrzosek is a member of Lex Super Omnia, which is a group comprised of prosecutors working for the independence of the office of the prosecutor. She was investigating the safety of conducting Presidential elections 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 power of the PiS Prosecutor General, Zbigniew Ziobro, to elect not to prosecute certain cases or to remove subordinate prosecutors from files<sup>40</sup>. It was upon Wrzosek's return to Warsaw that she was targeted with spyware. The Polish authorities followed the pattern of declining to confirm or deny their responsibility<sup>41 42</sup>.

### **Other Possible Targets**

#### **Supreme Audit Office**

---

<sup>36</sup> 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.

<sup>37</sup> The Guardian, '[More Polish opposition figures found to have been targeted by Pegasus spyware](#)', 17 February, 2022.

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

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

<sup>40</sup> European Commission Rule of Law 2022 Report, Poland Specific Chapter, [https://ec.europa.eu/info/sites/default/files/48\\_1\\_194008\\_coun\\_chap\\_poland\\_en.pdf](https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf) at pg. 16.

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

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

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 body<sup>43</sup> 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 party<sup>44</sup>.

### **PiS Associates**

19. It is believed by some 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. Adam Hofman, former PiS party spokesperson also alleges that his own colleagues 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<sup>45</sup> <sup>46</sup>. 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.

### **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 half and half 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.

### *I.B. Hungary*

21. Hungary was one of the first countries to be 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 confirmed by Amnesty International<sup>47</sup> that over 300 Hungarians have fallen victim to Pegasus, including political activists, journalists, lawyers, entrepreneurs and a former government minister<sup>48</sup>.

### **Purchase of Pegasus**

---

<sup>43</sup> <https://www.nik.gov.pl/en/about-us/>

<sup>44</sup> Politico, <https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/>, 18 January 2022.

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

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

<sup>47</sup> Euractiv, [Hungary employed Pegasus spyware in hundreds of cases, says government agency](#), 1 February 2022.

<sup>48</sup> DW, [‘Pegasus scandal: In Hungary, journalists sue state over spyware’](#), 29 January 2022.

22. The Hungarian Ministry of the Interior bought Pegasus from NSO Group in 2017 shortly after Orbán met with Polish Prime Minister Mateusz Morawiecki and former Israeli Prime Minister Benjamin Netanyahu<sup>49 50</sup>. The Hungarian Ministry of the Interior did not confirm this until 8 April 2021 when the Chair of the Parliamentary Defence and Law Enforcement Committee, Lajos Kósa, acknowledged the purchase of Pegasus by the Fidesz government<sup>51</sup> - Kósa still insisted however that the spyware has never been used against Hungarian citizens<sup>52</sup>.

## Legal Framework

23. The legal instruments governing spyware in Hungary are some of the weakest such provisions in Europe<sup>53 54</sup>. 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 ECtHR<sup>55</sup> despite the government's insistence that they have acted legally in all instances and are completely compliant with the law<sup>56 57</sup>. The *Act CXXV of 1995 on National Security Services* (hereinafter the Act) is currently governing the use of spyware in Hungary<sup>58</sup> 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.<sup>59</sup> The requirement to notify victims was unequivocally established in the case of *Klass and others v. Germany*<sup>60</sup> 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.

## Ex-ante Scrutiny

24. 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 the majority of instances, and on the judge designated by the President of the Budapest-

---

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

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

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

<sup>52</sup> DW, *Hungary admits to using NSO Group's Pegasus spyware*, 4 November 2021

<sup>53</sup> The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

<sup>54</sup> DW, *'Pegasus scandal: In Hungary, journalists sue state over spyware'*, 29 January 2022.

<sup>55</sup> 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.

<sup>56</sup> AP, <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>, 4 November 2021.

<sup>57</sup> Euractiv, *Hungary employed Pegasus spyware in hundreds of cases, says government agency*, 1 February 2022.

<sup>58</sup> Act CXXV of 1995 on National Security Services, [http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P\\_20200701\\_FIN.pdf](http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf).

<sup>59</sup> Act CXXV of 1995 on National Security Services, [http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P\\_20200701\\_FIN.pdf](http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf) at Section 58.

<sup>60</sup> *Klass and others v. Germany*, 6 September 1978, § 50, Series A no. 28. 40.

Capital Regional Court in some specific cases<sup>61 62</sup>. No appeal can be made against these decisions and there is virtually no oversight of the process<sup>63 64</sup>.

### **Ex-post Scrutiny**

25. In November 2021, at the insistence of the opposition, two committees in the Senate 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 representatives insisted that all surveillance was authorised through appropriate channels, but refused to comment as to whether or not journalists or politicians were targeted. 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.

### **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 proceedings in Hungary against both the State and the NAIH. The Hungarian Civil Liberties Union (HCLU) will represent 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 NSO Group<sup>65</sup>.

### **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 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.

### **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

---

<sup>61</sup> Act CXXV of 1995 on National Security Services, [http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P\\_20200701\\_FIN.pdf](http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf) at Sections 56-58.

<sup>62</sup> Europe's PegasusGate: Countering Spyware Abuse - EPRS Report, [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 pg. 20.

<sup>63</sup> Act CXXV of 1995 on National Security Services, [http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P\\_20200701\\_FIN.pdf](http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf) at Sections 57 and 58.

<sup>64</sup> European Commission Rule of Law Report 2022, [https://ec.europa.eu/info/sites/default/files/40\\_1\\_193993\\_coun\\_chap\\_hungary\\_en.pdf](https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf), at pg. 26.

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

numbers of over 300 persons were included in the findings of the Pegasus Project<sup>66</sup>. Among those were at least five journalists, ten lawyers and an opposition politician as well as activists and high profile business owners<sup>67</sup>. While the appearance of phone numbers on this list does not necessarily mean that hacking of those phones took place, 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.

### **Szabolcs Panyi**

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

### **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 party.

### **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 studies<sup>68</sup>. After attending a protest in Budapest, Beauduin was arrested in what is seen as a highly politically motivated move, and faced charges for assault of a police officer, which he vehemently denies<sup>69</sup>. It was reported that there was essentially no evidence against Beauduin, and the evidence that was submitted had been copied verbatim from the police testimony in another case<sup>70</sup>.

### **Ilona Patócs**

---

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

<sup>67</sup> The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests> , 18 July 2021 and Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/> , 19 July 2021.

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

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

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

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 case<sup>71</sup>. 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 it occurred. Her client, István Hatvani, had already served seven years for an assassination, which Patócs claims was a ‘politically motivated’ conviction<sup>72</sup>. Despite another party later claiming responsibility for the murder, the Hungarian Court of Appeal sent Hatvani back to prison to complete his original sentence. Many other lawyers’ phone numbers have been listed as potential targets of Pegasus, including President of the Hungarian Bar Association János Bánáti<sup>73</sup>. This targeting in particular shows a clear disregard from the government for the privilege that exists between lawyers and their clients.

### Other Targets

33. People inside the ruling party’s circle have also been targeted with spyware. It was reported by the independent Hungarian outlet Direkt36 in December 2021 that a bodyguard to János Áder, the President and close ally of Orbán, 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.

### Spyware Companies

34. The Hungarian government has not only purchased and utilised Pegasus spyware against its people, but it has been playing host to other companies in the intelligence market also. Black Cube is an Israeli private intelligence agency comprised of former employees of Mossad, the Israeli military and Israeli intelligence services<sup>74</sup>. Their own company website dubs them as a ‘creative intelligence service’ finding ‘tailored solutions to complex business and litigation challenges’<sup>75</sup>. Black Cube have been involved in a number of public hacking controversies including in the US and Romania<sup>76</sup>. Critically, it has also been uncovered that they are linked with 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.

### *I.C. Greece*

35. This year Greece has been shaken by a series of revelations regarding the evidently politically motivated use of spyware. On 26 July 2022, Member of the European

---

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

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

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

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

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

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

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<sup>77</sup>. The attempted infection with spyware was discovered during a check of Androulakis' phone by the European Parliament IT service<sup>78</sup>. 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. In September, it was revealed that former Minister of Infrastructure and lawmaker for the Syriza party, Christos Spirtzis<sup>79</sup>, had also been targeted with spyware. Furthermore, it was revealed later that month that Greece's National Intelligence Service (EYP) had allegedly targeted two of its own employees with spyware<sup>80</sup>. On 5 and 6 November, the Greek media revealed a list of 33 targets, all of whom were high profile personalities<sup>81</sup>, The list - if confirmed - reads like a stunning who is who of politics, business and media in Greece. The impact of this large-scale political use of spyware is infinitely bigger than just the people that appear on the list, as all their respective contacts and connections are indirectly 'caught' in the spying operation as well, including their contacts in EU bodies. The high prevalence of spyware was already visible in the 2021 Meta report, which mentions 310 fake websites links related to the Cytrox spyware company in its annex, 42 of which were set up to mislead targets in Greece alone<sup>82 83</sup>.

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.

## Purchase

---

<sup>77</sup> Euractiv. [EU Commission alarmed by new spyware case against Greek socialist leader.](#)

<sup>78</sup> Tagesspiegel. [Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.](#)

<sup>79</sup> Reuters. [One more Greek lawmaker files complaint over attempted phone hacking.](#)

<sup>80</sup> Efsyn. [Targeting the disliked.](#)

<sup>81</sup> Documento. [Apocalypse: They Watched - This Sunday in Document.](#)

<sup>82</sup> Meta. [Threat Report on the Surveillance-for-Hire Industry.](#)

<sup>83</sup> InsideStory. [Who was tracking the mobile phone of journalist Thanasis Koukakis?](#)

38. The government denies the purchase of Predator spyware<sup>84</sup>. 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. The hypothesis of private actors behind the Predator attacks is moreover highly implausible, as it would not explain the choice of targets.
39. Another possibility is that Predator was acquired through Ketyak, a special entity set up by former EYP boss Kontoleon. It operates at a distance from the EYP.
40. 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. 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.

### **Grigoris Dimitriadis**

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.

### **Felix Bitzios**

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 frozen<sup>85</sup>. Bitzios benefited from a legislative amendment introduced by Prime Minister Mitsotakis soon after he came to power in 2019. The controversial amendment set a time limit on the freezing of assets, thus enabling the release of frozen assets after a maximum of eighteen months<sup>86</sup>. Thanks to the amendment of the Mitsotakis government, the assets of Bitzios could be released.
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 Intellexa<sup>87</sup>. 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.

---

<sup>84</sup> Euractiv. [EU Commission alarmed by new spyware case against Greek socialist leader.](#)

<sup>85</sup> Lexocology. [Cyprus court offers directions to bank on ambit of freezing injunction.](#)

<sup>86</sup> Financial Times. [Greek law change viewed as backtracking on money laundering.](#)

<sup>87</sup> Inside Story. [Predatorgate: The second shareholder of Intellexa SA.](#)

Nevertheless, Bitzios had been connected to Intellexa from March 2020 to June 2021 as a deputy administrator.

### **Giannis Lavranos**

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

### **Intellexa**

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 Ministry of Foreign Affairs in Greece, responsible for the distribution of export permits, declared that no export licenses were granted to the Intellexa group of companies<sup>88</sup>. However, Intellexa companies based in Greece reportedly exported their products to Bangladesh and at least one Arab country<sup>89 90</sup>. For a detailed description on Intellexa see the chapter on the Spyware Industry.

### **Krikel**

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 Mexal<sup>91</sup>. 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.
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 Protection<sup>92</sup>. 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 throughout<sup>93</sup>. Krikel became an important supplier of the Greek Ministry of Citizen

---

<sup>88</sup> Inside Story. [Who signs the exports of spyware from Greece and Cyprus?](#)

<sup>89</sup> Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

<sup>90</sup> Inside Story. [Who signs the exports of spyware from Greece and Cyprus?](#)

<sup>91</sup> 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 \[Revealing documents\]](#).

<sup>92</sup> Inside Story. [Predatorgate's invisible privates](#).

<sup>93</sup> Inside Story. [Predatorgate's invisible privates](#).

Protection. Since 2018, it signed seven contracts with the Greek government, six of which are secret<sup>94</sup>.

48. Krikel company also became the local representative of Italian company RCS Lab. In June 2021, the EYP purchased a wiretapping system from RCS lab<sup>95</sup> through Krikel<sup>96</sup>. 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 problem<sup>97</sup>. Other sources however claimed that Kontoleon ordered the destruction of files on 29 July 2022<sup>98</sup>.
49. Interestingly employees of Krikel have been spotted working at Ketyak, allegedly ‘pro bono’. Ketyak has apparently been granted €40 million from the RRF, through a confidential tender procedure based on a secret decision of the Prime Minister.

### **Involvement of Bitzios and Lavranos**

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 2017<sup>99</sup>. 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)<sup>100</sup>.
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.

### **Legal Framework**

52. Greece has a fairly robust legal framework in principle. However, legal amendments have weakened crucial safeguards and political appointment to key positions are an obstacle to scrutiny and accountability.

### **Ex-ante scrutiny**

---

<sup>94</sup> InsideStory. [Predatorgate’s invisible privates.](#)

<sup>95</sup> Hellas Posts English. [The EYP supplier contaminates smartphones in Greece as well.](#)

<sup>96</sup> TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

<sup>97</sup> TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

<sup>98</sup> Euractiv. [Greek MEP spyware scandal takes new turn.](#)

<sup>99</sup> TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

<sup>100</sup> InsideStory. [From Koukakis to Androulakis: A new twist in the Predator spyware case.](#)

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 Code<sup>101</sup>.

### Act of Legislative Content

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 governor<sup>102</sup>. However, as the governing party currently has an absolute majority in the Parliament's Special Permanent Committee on Institutions and Transparency, it endorsed the nomination of Mr Demiris as new EYP governor, whilst all other opposition parties were against<sup>103</sup>. Incidentally, 2nd deputy commander of the EYP is Dionysis Melitsiotis<sup>104</sup>, a former member of the private office of the Prime Minister, and another Deputy Director is Anastasios Mitsialis, a former Nea Demokratia official<sup>105</sup>.

### Ex-post scrutiny

55. Since 2019, the actions of the EYP have been under the direct control of Prime Minister Kyriakos after a change in the law following the victory of New Democracy in 2019<sup>106</sup>.
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 compromised<sup>107</sup>. The right of an individual to have access to information on whether the person in question has been the object of surveillance is outlined in Law 2472/1997<sup>108</sup>. 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 communications<sup>109</sup>. This de facto strips the individual of its right to information. The amendment was introduced in a highly irregular manner. It was added to a totally unrelated law (a bill to do with covid

---

<sup>101</sup> ICLG. [Cybersecurity Laws and Regulation Greece 2022](#).

<sup>102</sup> Efsyn. [What \(does not\) change with the Act of Legislative Content for EYP](#).

<sup>103</sup> Kathemirini. [Themistoklis Demiris: His appointment to the management of EYP was approved by a majority](#).

<sup>104</sup> Ekathimerini. [National security takes center stage](#).

<sup>105</sup> Greek City Times. [Greek PM appoints new security and intelligence chiefs](#).

<sup>106</sup> Euractiv. [Another Greek opposition lawmaker victim of Predator](#).

<sup>107</sup> Constitutionalism. [Contradiction of article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications](#).

<sup>108</sup> Dpa. [Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data](#).

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

measures) and the deadlines required by the Constitution were not respected<sup>110 111 112</sup>. There was therefore no proper consultation process.

57. The possibilities for ex-post scrutiny are further weakened by the fact that Greece has still not fully implemented the EU Whistleblowers Directive<sup>113</sup>.

### **Public scrutiny**

58. Greece ranks lowest of all EU countries in the World Press Freedom Index 2022: 108 out of 180<sup>114</sup>. In 2021, journalist Giorgos Karaivaz was murdered. The murder has still not been resolved. Journalists face intimidation and SLAPPS. Grigoris Dimitriadis<sup>115</sup> launched Strategic Lawsuits against Public Participation (SLAPPS) against news outlets Reporters United and Efimerida ton Syntakton (EfSyn)<sup>116</sup> after he was forced to resign. Government Minister Oikonomou sought to discredit a Politico reporter, Nektaria Stamouli, by implying that her articles about the spyware scandal were politically motivated<sup>117</sup>. Indeed two of the Predator victims, 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 Triantafyllou reported about the spyware scandal, and they were allegedly put under surveillance<sup>118</sup>.

### **Redress**

#### **The National Transparency Authority**

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 involved<sup>119</sup>.
60. The EAD report concluded that both the EYP and the Ministry of Citizen Protection had not concluded contracts with Intellexa and other related national companies. They also had not purchased or used the Predator spyware<sup>120</sup>. However, the EAD did not investigate the bank accounts of Intellexa and Krikel, nor the affiliated offshore companies. In addition, the NTA only visited the offices of Intellexa and Krikel after

---

<sup>110</sup> Hellenic Parliament. [Constitution](#).

<sup>111</sup> Hellenic Parliament. [Rules of Procedure of the House](#).

<sup>112</sup> Govwatch. [Violation of the legislative process for amendments in law 4790/2021](#).

<sup>113</sup> [https://ec.europa.eu/commission/presscorner/detail/EN/inf\\_22\\_3768](https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768)

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

<sup>115</sup> Tagesspiegel. .

<sup>116</sup> EUobserver. [Greece accused of undermining rule of law in wiretap scandal](#).

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

<sup>118</sup> Heinrich-Böll-Stiftung. [In conditions of absolute loneliness](#).

<sup>119</sup> InsideStory. [From Koukakis to Androulakis: A new twist in the Predator Spyware case](#).

<sup>120</sup> InsideStory. [From Koukakis to Androulakis: A new twist in the Predator Spyware case](#).

2 months, at which point employees were working home due to COVID. The EAD furthermore did not meet with legal representatives of the companies in question.<sup>121</sup>.

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 pushbacks<sup>122</sup>. The Director of EAD, a former employee of Mitsotakis, did not meet with PEGA during the mission in November 2022.

### **The Hellenic Authority for Communication Security and Privacy (ADAE)**

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.

### **The Committee on Institutions and Transparency**

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 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 spyware<sup>123</sup>.

### **The Parliamentary Committee of Inquiry**

64. A proposal by the PASOK-KINAL party to set up a committee of inquiry into the alleged use of spyware<sup>124</sup> was endorsed by 142 MPs of the opposition, while the 157 Nea Demokratia MPs abstained<sup>125</sup>. 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.
65. The government majority in the committee refused to invite Bitzios and Lavranos, but it did invite Stamatis Tribalis - current manager of Krikel - and Sara Hamou. On 22 September, Tribalis testified in front of this parliamentary committee. Tribalis presented blatantly false information about the involvement of Bitzios and Lavranos in Krikel, claiming *i.a.* that he himself was the owner of Krikel<sup>126</sup>.

---

<sup>121</sup> InsideStory. [From Koukakis to Androulakis: A new twist in the Predator Spyware case.](#)

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

<sup>123</sup> Reuters. [Greek intelligence service admits spying on journalist - sources.](#)

<sup>124</sup> Tovina. [Interceptions: Committee of Inquiry to monitor Androulakis - Pasok's proposal in detail.](#)

<sup>125</sup> Tovina. [Parliament: The examination for the attendances from 2016 was passed - With 142 'yes'.](#)

<sup>126</sup> TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

66. One witness, Sarah Hamou of Intelexa, 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, each party published its own report. Some 5 500 pages of documents, including the minutes and the deposition of Hamou have been classified, although it is entirely within the powers of Parliament to declassify them. Quite paradoxically, the inquiry committee thus serves to shield information, instead of providing access to it.

### **The Targets**

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.

### **Thanasis Koukakis**

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 government impeding the prosecution of money laundering and other financial wrongdoing (indeed the retroactive effect led to twelve pending cases being dropped)<sup>127</sup>. 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.

### **Nikos Androulakis**

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 telephone<sup>128</sup>. 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 him<sup>129</sup>.
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

---

<sup>127</sup> Inside Story. Who was tracking the mobile phone of journalist Thanasis Koukakis.

<sup>128</sup> InsideStory. [From Koukakis to Androulakis: A new twist in the Predator spyware case.](#)

<sup>129</sup> Euractiv. [EU Commission alarmed by new spyware case against Greek socialist leader.](#)

Premiership of Mitsotakis. Another candidate, Andreas Loverdos, had served earlier as a Minister in a Nέα 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 Nέα 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.

### **Stavros Malichoudis**

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<sup>130</sup> <sup>131</sup>. 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 Kos<sup>132</sup>.

### **Christos Spirtzis**

72. On 15 November 2021, former Minister of Infrastructure and lawmaker for the Syriza party Christos Spirtzis was targeted with the Predator spyware on his mobile phone<sup>133</sup>.

### **Tasos Telloglou, Eliza Triantafyllou and Thodoris Chondrogiannos**

73. Tasos Telloglou and Eliza Triantafyllou have allegedly been spied upon during their investigative work for the Inside Story.

### **Other targets**

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<sup>134</sup>. Mr Oikonomou - government spokesperson - has stated that the article lacks concrete evidence<sup>135</sup>.
75. On 5 and 6 November 2022 Documento reported on a list containing 33 names of persons targeted with Predator spyware<sup>136</sup>. Among them 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 revelations of the list are highly disturbing not just because of the high profile names on it, but also

---

<sup>130</sup> Efsyn. Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ

<sup>131</sup> Solomon. Solomon's reporter Stavros Malichoudis under surveillance for 'national security reasons'.

<sup>132</sup> BalkanInsight. [Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.](#)

<sup>133</sup> Ekathimerini. [Former SYRIZA minister says he was targeted by Predator.](#)

<sup>134</sup> Ta Nea. [Four illegal manipulations by suspicious center.](#)

<sup>135</sup> Politico. [Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.](#)

<sup>136</sup> Documento, edition 6 November 2022.

because it suggests that the abuse of spyware is systematic, large-scale, and part of a political strategy.

#### *I.D. Cyprus*

76. 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. 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.
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.
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. Cyprus is a popular destination for many Israeli spyware companies.

### **Legal Framework**

#### **Dual-Use Regulation**

79. Compared to its legal framework in place, Cyprus is reportedly rather lenient in providing spyware companies with export licenses<sup>137</sup>. Companies use tricks to circumvent the rules. That is, the physical hardware of the product is sent to a recipient country without the software loaded on it<sup>138</sup>. 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 country<sup>139</sup>. Another way is to state that the product is exported for demonstration purposes only, although a detailed description of the product is added<sup>140</sup>.
80. Many Israeli companies come to Cyprus to start off their European activity<sup>141</sup>. Different sources reported furthermore that the country is home to approximately 29 Israeli companies<sup>142</sup>. 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 NSO<sup>143</sup> as well as spyware materials from WiSpear<sup>144</sup>.

---

<sup>137</sup> InsideStory. [Who signs the exports of spyware from Greece and Cyprus?](#)

<sup>138</sup> InsideStory. [Who signs the exports of spyware from Greece and Cyprus?](#)

<sup>139</sup> Philenews. [This is how interception patents are exported from Cyprus.](#)

<sup>140</sup> Philenews. [Export of monitoring software confirmed.](#)

<sup>141</sup> Philenews. [Revelations in Greece: Predator came from Cyprus.](#)

<sup>142</sup> Makarios Drousiotis. [Κράτος Μαφία](#). Chapter 6. Published 2022

<sup>143</sup> Makarios Drousiotis. [Κράτος Μαφία](#). Chapter 6. Published 2022.

<sup>144</sup> Inside Story. [Predator: The 'spy' who came from Cyprus.](#)

## Ex-ante scrutiny

81. The law on the Protection of the Confidentiality of Private Communications 92(I)/1996 stipulates that the application for authorisation to monitor private communication must be submitted to the Court<sup>145</sup>.

## Ex-post scrutiny

82. On paper, violating the protection of private communications is a de jure criminal offense. De facto, this illegality is often hidden behind the invocation of national security<sup>146</sup>. There is no legislature 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 unchecked<sup>147</sup>.

## Redress

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 President<sup>148</sup>.

## 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 2017<sup>149</sup>. Tal Dilian served in different leadership positions in the Israeli Defence Force for 25 years before he retired from the military in 2002<sup>150</sup>. 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 Ltd<sup>151</sup>.
85. In Cyprus, Dilian got closely associated with Abraham Sahak Avni. Avni has formerly been involved in the Israeli Police Special Forces as special detective<sup>152</sup>. In November 2015, he acquired Cypriot citizenship and a golden passport because of a 2.9 million euro investment in real estate<sup>153</sup>. Avni founded the Cypriot NCIS Intelligence Services ltd<sup>154</sup>, a company that was reportedly involved with the most powerful technology-

---

<sup>145</sup> CyLaw. [The Protection of Privacy of Private Communications \(Interception and Access to Recorded Private Communications Content\) Law of 1996 \(92\(I\)/1996\)](#)

<sup>146</sup> Makarios Drousiotis. [Κράτος Μαφία..](#) Chapter 6. Published 2022.

<sup>147</sup> Philenews. [Legal but uncontrolled interceptions.](#)

<sup>148</sup> Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

<sup>149</sup> 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>

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

<sup>151</sup> Opencorporates. [Passitora ltd.](#)

<sup>152</sup> ShahakAvni. [About Shahak Avni.](#)

<sup>153</sup> Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

<sup>154</sup> Philenews. [FILE: The state insulted Avni and Dilian.](#)

oriented companies in the world<sup>155</sup>. 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 2016<sup>156</sup>. Government Party DISY (Dimokratikós Sinagermós) is also part of the company's clientele. Reportedly, Avni had installed security equipment in the party's offices<sup>157</sup>. Next to Avni's security equipment, Dilian's materials were also sold to the Cyprus Drug Enforcement Agency and the Cypriot Police<sup>158</sup>.

86. The connections between Dilian and Avni are numerous. Dilian's company WiSpear shared a building in Lacarna and some of its personnel with Avni<sup>159</sup>. 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<sup>160</sup> and is also part of Intellexa Alliance. Reportedly, Avni's relations with the DISY party created the testing ground for Dilian's products<sup>161</sup>.

### **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'<sup>162</sup>. 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<sup>163</sup>. More detailed information on the corporate structure in the chapter on the Spyware Industry.
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 were allegedly provided with top functions at Intellexa<sup>164</sup>. 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'<sup>165 166</sup>.
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 2011<sup>167</sup> and was

---

<sup>155</sup> Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

<sup>156</sup> Philenews. [FILE: The state insulted Avni and Dilian.](#)

<sup>157</sup> Tovima. [The unknown "bridge" between Greece and Cyprus for the eavesdropping system.](#)

<sup>158</sup> Inside Story. [Predator: The "spy" who came from Cyprus.](#)

<sup>159</sup> Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

<sup>160</sup> CyprusMail. [Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.](#)

<sup>161</sup> Inside Story. [Predator: The "spy" who came from Cyprus.](#)

<sup>162</sup> <https://intellexa.com/>

<sup>163</sup> Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

<sup>164</sup> Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

<sup>165</sup> Makarios Drousiotis. [Κράτος Μαφία](#). Chapter 6. Published 2022.

<sup>166</sup> Philenews. [Export of tracking software from Cyprus.](#)

<sup>167</sup> Politis. ["Interceptions" file: Classified Police Report \(2016\) shows he knew everything about Avni](#)

registered with the assistance of the former law firm of Savvas Angelides<sup>168</sup>. Their partnership however dissolved in 2012. Nevertheless, Savvas Angelides was the person in charge of controlling Avni and Dillian in the case of the surveillance van<sup>169</sup>.

90. Opposition party AKEL expressed outrage over the cases against Dillian and staff being dropped, and denounced the legal decision as a cover-up by the Attorney General<sup>170</sup>. After all, the Cypriot government had reportedly purchased equipment from Dillian's company and one of the accused employees had allegedly worked for NSO, providing the KYP with instructions on how to use the Pegasus spyware<sup>171</sup>. Dropping the charges ensured that the information on the links between Dillian's company and the Cypriot government would remain protected<sup>172</sup>. 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 influenced by governmental interventions, leaving the individual victim defenceless.

### The move to Greece

91. Following the episode of the van and the lawsuit, Dillian moved Intellexa's operations to Greece, although he never left Cyprus and is still a resident. Indirect links between several natural and legal persons as registered in Cyprus and Greece expose the facilitation of Dillian's businesses to Athens<sup>173</sup>.
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 Dillian and Avni<sup>174</sup>. 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-Chairman<sup>175</sup>. 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 DISY<sup>176</sup>.

### NSO Group and Cyprus

93. Next to Intellexa Alliance, Cyprus was allegedly also home to NSO Group. In 2010 Tal Dillian, together with Boaz Goldman and Eric Banoun, launched the company Circles

---

<sup>168</sup> Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022.

<sup>169</sup> Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

<sup>170</sup> Financial Mirror. [Anger after 'spy van' charges dropped](#).Le

<sup>171</sup> Makarios Drousiotis. [Κράτος Μαφία..](#) Chapter 6. Published 2022.

<sup>172</sup> Makarios Drousiotis. [Κράτος Μαφία..](#) Chapter 6. Published 2022.

<sup>173</sup> Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.

<sup>174</sup> Tovima. [The unknown "bridge" between Greece and Cyprus for the eavesdropping system.](#)

<sup>175</sup> EDS. [2003/2004 Bureau.](#)

<sup>176</sup> Tovima. [The unknown "bridge" between Greece and Cyprus for the eavesdropping system.](#)

Technologies, specialised in the sale of systems that exploit SS7 vulnerabilities<sup>177</sup>. 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, 2016<sup>178</sup>.

94. The denial by the Cypriot government of the Pegasus export and development in the country seems however incorrect. On 21 June 2022, NSO official Chaim Gelfad did state that NSO companies in Cyprus and Bulgaria are engaged in software providing intelligence services<sup>179</sup>. 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 issued an invoice of 7 million dollars for services to the company in question<sup>180</sup>.
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<sup>181 182</sup>. 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 surveiling him and his near ones with Pegasus.

### **Black Cube**

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 Cyprus<sup>183</sup>.

### **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.

### **Victim Makarios Drousiotis**

---

<sup>177</sup> Amnesty International. Operating from the Shadows.

<sup>178</sup> Amnesty International. Operating from the Shadows.

<sup>179</sup> Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

<sup>180</sup> Akel report. PEGA mission to Cyprus.

<sup>181</sup> Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.

<sup>182</sup> Haaretz. Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals.

<sup>183</sup> The New Yorker. How Democracies Spy on their Citizens.

98. Starting at February 2018, investigate journalist Makarios Drousiotis was allegedly spied on by the Cypriot government. 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<sup>184</sup>.

### **Additional remarks**

99. Cyprus appears to have 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. 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.

### *I.E. Spain*

100. The July 2021 revelations by the Pegasus project showed a large number of 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 Prime Minister Pedro Sanchez, Minister for Defence Margarita Robles and Minister of the Interior Fernando Grande-Marlaska, similarly to the case of the French President and government ministers<sup>185</sup>. The targeting of a second group of victims is referred to as ‘CatalanGate’<sup>186</sup>. It includes Catalan parliamentarians, Members of the European Parliament, lawyers, civil society organisation members and some family and staff connected to those victims<sup>187</sup>. The ‘CatalanGate’ surveillance scandal was first reported on in 2020, but it was not until April 2022 that Citizen Lab completed their in-depth investigation that the scale of the scandal was revealed. The results of that probe showed that at least 65 persons were targeted<sup>188</sup>. In May 2020, the Spanish authorities admitted to targeting 18 of those 65 victims with court authorisation<sup>189</sup>.

### **Purchase of Spyware**

101. The past purchase of various spyware products like SITEL in 2001 and the spyware of Hacking Team in 2010 by the Ministry of the Interior, the Spanish National Intelligence

---

<sup>184</sup> Makarios Drousiotis. *Κράτος Μαφία*. Chapter 5. Published 2022.

<sup>185</sup> 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](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.

<sup>186</sup> Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022.

<sup>187</sup> 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.

<sup>188</sup> 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.

<sup>189</sup> El National, [https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge\\_752448\\_102.html](https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html), 5 May 2022.

Centre (CNI) and police has been widely publicised<sup>190</sup>. It was also previously reported by CitizenLab that Spain was a suspected customer of Finfisher<sup>191</sup>. In 2020, the Spanish newspaper *El Pais* reported that Spain has done business with NSO Group and that the CNI routinely uses Pegasus<sup>192</sup>. The Spanish government allegedly purchased the spyware in the first half of the 2010s for an estimated amount of €6 million<sup>193 194</sup>. In addition, a former employee of NSO has further confirmed that Spain has an account with the company despite the Spanish authorities declining to comment or confirm<sup>195</sup>.

## Legal Framework

102. The right to privacy is protected under Article 18 of the Spanish Constitution of 1978, including the right to secrecy in ‘postal, telegraphic and telephone communication’<sup>196</sup>. The use of spyware such as Pegasus and Candiru is a violation of Article 18; however, there is an exception to this right in the case of a court granting authorisation<sup>197</sup>. The constitution also provides further exceptions to those rights in Part I Section 55 by stating that some freedoms are eligible to be suspended with ‘participation of the courts and proper parliamentary control’ in the case of individuals under investigation for activities relating to armed groups or terrorist organisations<sup>198</sup>.
103. The Spanish intelligence service is made up of three main agencies. Firstly, the National Intelligence Service (CNI) which is under the control of the Ministry of Defence. The Director of the CNI is nominated by the Minister for Defence and serves as the Prime Minister’s lead advisor on issues relating to intelligence and counter-intelligence<sup>199</sup>. 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<sup>200 201</sup>.

## Ex-ante Scrutiny

---

<sup>190</sup> 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.

<sup>191</sup> 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.

<sup>192</sup> 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.

<sup>193</sup> Politico, <https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/>, 20 April 2022.

<sup>194</sup> 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.

<sup>195</sup> The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

<sup>196</sup> Constitution of Spain 1978,

[https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo\\_primero.aspx](https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx), at Section 18.

<sup>197</sup> Constitution of Spain 1978,

[https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo\\_primero.aspx](https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx), at Section 18.

<sup>198</sup> Constitution of Spain 1978,

[https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo\\_primero.aspx](https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx), at Section 55.

<sup>199</sup> <https://www.cni.es/en/intelligence>

<sup>200</sup> [https://emad.defensa.gob.es/en/?\\_locale=en](https://emad.defensa.gob.es/en/?_locale=en)

<sup>201</sup> Geneva Centre for Security Sector Governance report 2020, [https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence\\_jan2021.pdf](https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf) at pg. 40.

104. 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 past<sup>202</sup>. The CNI was established under Law 11/2002 May 6 and it authorises the CNI to conduct ‘security investigations’<sup>203</sup>. However, there is little clarification on the means or limitations of such activities<sup>204</sup>. Law 11/2002 also established parliamentary, executive and legislative oversight control over the CNI<sup>205</sup>. Parliamentary oversight is to be carried out by the Official Secrets Committee of the Spanish Congress, which was established in 1995<sup>206</sup>. The Delegated Committee for Intelligence Affairs is in executive control of the body, and co-ordinates the intelligence activities of the CNI<sup>207</sup>. Lastly, the Defence Committee of the Congress of Deputies conducts legislative oversight over the CNI<sup>208</sup>. The annual Intelligence Directive dictates the intelligence priorities of the CNI for the year<sup>209</sup>.

### Ex-post Scrutiny

105. The laws establishing the CNI also established the Defence Committee of the Congress of Deputies and it is responsible for allocating the confidential 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 transparency<sup>210</sup>.

106. The Official Secrets Committee is required to submit an annual report on the activities of the intelligence services, however when it was convened as a result of the surveillance by the CNI, it was the first meeting of the body in more than two years. Head of the CNI Paz Esteban appeared before the Committee on 5 May 2022 to present the court authorisations for the 18 victims that the authorities have taken responsibility

---

<sup>202</sup> 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.

<sup>203</sup> 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.

<sup>204</sup> OMCT, <https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain>, 4 May 2022.

<sup>205</sup> 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.

<sup>206</sup> Law 11/1995 May 11, <https://www.boe.es/eli/es/l/1995/05/11/11/con>.

<sup>207</sup> 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.

<sup>208</sup> 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.

<sup>209</sup> 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.

<sup>210</sup> 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.

for targeting.<sup>211</sup> The hearing was not public and those present were not allowed to enter with any electronic on them whatsoever<sup>212</sup>.

## Public Scrutiny

107. There has been a significant amount of public scrutiny on the ‘CatalanGate’ scandal 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 victims. Inversely, some Spanish politicians have tried to discredit CitizensLab, suggesting their methods are unsound or that they are politically motivated. A collaborator of CitizensLab, himself of Catalan origin, was among the targets, along with his parents, who are not politically active at all<sup>213</sup>.

## Redress

108. A legal case regarding the surveillance of Prime Minister Sanchez and Minister for Defence Robles was filed in Madrid in the Audiencia Nacional, the Spanish National Court (SNC), by the state solicitors’ office<sup>214</sup>. Judge Jose Luis Calama, head of the Central Court of Instruction number 4, is responsible for this on-going case<sup>215</sup>. 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 Ministers<sup>216</sup>.

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 Catalan victims of spyware are moving at a slow pace<sup>217 218</sup>. The first case in Investigative Court number 32 in Barcelona was filed by two Pegasus victims in 2020; former President of the Catalanian 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<sup>219</sup>. Andreu Van Den Eynde is one of the lawyers representing Torrent and Maragall in this case, and is a victim of Pegasus himself. Van Den Eynde has criticised the courts consistently delaying proceedings and

---

<sup>211</sup> El Nacional, [https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge\\_752448\\_102.html](https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html), 5 May 2022.

<sup>212</sup> El Nacional, [https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge\\_752448\\_102.html](https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html), 5 May 2022.

<sup>213</sup> Dit Kan Geen Toeval Zijn, De Volkskrant podcast series by Huib Modderkolk and Simone Eleveld, 2022.

<sup>214</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

<sup>215</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

<sup>216</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

<sup>217</sup> El Diario, [https://www.eldiario.es/catalunya/juez-barcelona-no-ve-base-imputar-empresa-pegasus-espionaje\\_1\\_9068271.html](https://www.eldiario.es/catalunya/juez-barcelona-no-ve-base-imputar-empresa-pegasus-espionaje_1_9068271.html), 9 June 2022.

<sup>218</sup> El Diario, [https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados\\_1\\_9037282.html](https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html), 30 May 2022.

<sup>219</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

virtually ‘paralysing’ the case<sup>220</sup>. Omnium Cultural and the Popular Unity Candidacy party (CUP) have also filed a case in the same court in Barcelona. Lawyer Benet Salellas, who is involved in both cases, is asserting that the Spanish government is behind the targeting<sup>221</sup>.

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 unified<sup>222</sup>. In other words, the cases of the victims from the Spanish government and the ‘CatalanGate’ victims would all be heard in the SNC in Madrid. The lawyers representing the Catalan victims assert that there is no link between the cases unless the perpetrator is proved to be the same in all instances of surveillance<sup>223</sup>.
111. There are a number of other pending legal cases linked to the 65 Catalan victims. One such case was filed by lawyer and Pegasus victim Gonzalo Boye on behalf of at least 19 victims against NSO, its three founders Niv Karmi, Shalev Hulio and Omri Lavie, Q Cyber Technologies, and OSY, a subsidiary company based in Luxembourg<sup>224</sup> <sup>225</sup>. 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 Luxembourg<sup>226</sup>.

## Targets

112. The targeting of Catalan citizens with spyware reportedly began as early as 2015, and has been carried out on a large scale since 2017<sup>227</sup>. 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 question<sup>228</sup>.
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 2021<sup>229</sup>. There is little information available so far on details of this

---

<sup>220</sup> El Diario, [https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados\\_1\\_9037282.html](https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html), 30 May 2022.

<sup>221</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

<sup>222</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

<sup>223</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

<sup>224</sup> El Nacional, [https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus\\_751530\\_102.html](https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html), 3 May 2022.

<sup>225</sup> Catalan News, <https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab>, 19 April 2022.

<sup>226</sup> Catalan News, <https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab>, 19 April 2022.

<sup>227</sup> <https://catalonia.citizenlab.ca/#targeting-puigdemont>

<sup>228</sup> 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.

<sup>229</sup> El Nacional, [https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience\\_750840\\_102.html](https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html), 2 May 2022.

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. 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<sup>230</sup>. Grande-Marlaska was infected on his personal device<sup>231</sup>. 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 confirmed<sup>232</sup>.

114. In total, 65 Catalonians were confirmed to have been targeted with mercenary spyware, 63 with Pegasus, four with Candiru and at least two people were targeted by both<sup>233</sup>. At least 51 individuals were successfully infected<sup>234</sup>. 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 targeted<sup>235</sup>. The majority of those 18 persons were never charged with a crime, and yet were included on this list. Minister for Defence Robles has relied heavily on the Official Secrets Act rather than expand on what were the reasons for the surveillance of those specific targets<sup>236</sup>. All 65 Catalan targets have at some point in time been in contact with the Catalan separatists living outside Spain.

### **Members of the European Parliament**

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 targeting<sup>237</sup>: Diana Riba i Giner, Antoni Comín i Oliveres, Jordi Solé, Carles Puigdemont, and Clara Ponsati.

### ***Catalonian Politicians***

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

---

<sup>230</sup> The Economist, <https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099>, 7 May 2022.

<sup>231</sup> La Razon,

<sup>232</sup> The Economist, <https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099>, 7 May 2022.

<sup>233</sup> 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.

<sup>234</sup> 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.

<sup>235</sup> El Nacional, [https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge\\_752448\\_102.html](https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html) 5 May 2022.

<sup>236</sup> El Nacional, [https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge\\_752448\\_102.html](https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html) 5 May 2022.

<sup>237</sup> 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.

2019 WhatsApp Pegasus infections<sup>238</sup>. 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 Pegasus<sup>239</sup>. All of the Presidents of Catalonia since 2010 have been targeted with spyware either during or after their term in office<sup>240</sup>. 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.

## Civil Society Organisations

117. Jordi Domingo was one of the first Catalan activists that was reported to be targeted in 2020. Though a supporter of Catalan independence, 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 constitution of Catalonia<sup>241</sup>.

## Lawyers

118. Gonzalo Boye has represented many high profile Catalan figures, including former Presidents Puigdemont and Torras<sup>242</sup>. Over five months between January and May of 2020, he was a victim of Pegasus himself<sup>243</sup>. Boye was targeted as many as 18 times during that period via text messages that appeared as tweets from civil society organisations or prominent news outlets<sup>244</sup>. CitizenLab confirmed at least one successful infection on 30 October 2020. The infection came just 48 hours after the arrest of one of his clients<sup>245</sup>. The targeting of Boye has called in to question the legality of attacking the lawyer-client privilege.

119. Andreu van den Eynde i Adroer, was successfully infected with Pegasus on 14 May 2020<sup>246</sup>. The hacking occurred while he was acting as the lawyer of both Raul Romeva and Oriol Junqueras in their case before the Supreme Court.

---

<sup>238</sup> The Guardian, <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>, 13 July 2020.

<sup>239</sup> 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.

<sup>240</sup> 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/>

<sup>241</sup> The Guardian, <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>, 13 July 2020.

<sup>242</sup> <https://catalonia.citizenlab.ca/>

<sup>243</sup> <https://catalonia.citizenlab.ca/>

<sup>244</sup> <https://catalonia.citizenlab.ca/>

<sup>245</sup> <https://catalonia.citizenlab.ca/>

<sup>246</sup> 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.

120. Similarly, prominent 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.

#### *I.F. Other Member States*

121. National authorities have so far shared very little official information about the acquisition and use of spyware in their countries, nor about the budgetary aspects or legal framework governing it. Vendors and countries issuing export licenses (in particular Israel) share no information about the customers. Only Austria, Poland, Cyprus have responded to the questionnaire sent by PEGA on 15 July 2022, but mostly in a very general, even evasive way.
122. But by putting together information from various sources, a partial image can be reconstructed, and issues can be identified that raise concern and merit further investigation.
123. It can be safely assumed that authorities in all Member States use spyware in one way or another. 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. 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.
124. From information provided by NSO Group, we know that Pegasus was sold in at least fourteen EU countries, until the contracts with two countries were terminated. It is not known 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.
125. 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<sup>247</sup>. 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<sup>248</sup>.
126. 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.
127. Spyware is clearly also used by law enforcement, not just by intelligence agencies. There is no information about the material obtained with the use of spyware, and how that can be, and has been used to detect, investigate, and prosecute crime in the context of EU police and justice cooperation. There are big question marks over the

---

<sup>247</sup> <https://wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf>

<sup>248</sup> [https://www.issworldtraining.com/iss\\_europe/sponsors.html](https://www.issworldtraining.com/iss_europe/sponsors.html)

admissibility in court of such material as evidence in the context of EU police and justice cooperation, including within Europol and Eurojust.

## **The Netherlands**

128. The 2017 coalition agreement of the Dutch government states that the Dutch police 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 has to ask the provider whether it has provided to EU- or UN-sanctioned countries and performs a check if the country where the provider is based has an export control regime where human rights are assessed in the export license procedure. This assessment is repeated periodically. It should be noted that this restriction only seems to apply to spyware acquisitions by the police. The intelligence services are not explicitly mentioned. According to the government, the police does use hacking software since 2019, although the authorities do not mention which type<sup>249</sup>. It would appear that NSO Group and its spyware product Pegasus do not meet the above-mentioned standards, in any case not before the tightening of the export regime of Israel in December 2021<sup>250</sup>. No insight is given into the expenditure by both police and intelligence services for the purchase and use of the spyware system.
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 spyware<sup>251</sup>. It is not clear whether or not the contract was signed and any spyware was provided to the Dutch Defence Ministry.

## **Belgium**

130. In an interview with *The New Yorker*, a former Israeli intelligence official revealed that the Belgian police uses Pegasus in its operations<sup>252</sup>. In response, the Belgian police stated ‘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 criminals<sup>253</sup>.

## **Germany**

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

---

<sup>249</sup> <https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/23/ntwoorden-op-kamervragen-over-het-gebruik-van-hacksoftware-zoals-pegasus-in-nederland>

<sup>250</sup> <https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021>

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

<sup>252</sup> <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>

<sup>253</sup> <https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spijonagetool-pegasus/10329450.html>

distinguishes two forms of spyware use<sup>254</sup>: access all information (Online-Durchsuchung<sup>255</sup>) and access only live communication (Quellen-TKÜ<sup>256</sup>). Since the original Pegasus software could access all information on a device, and not just live communication, its use by the BKA would violate the law. 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 so<sup>257</sup>. Only after new negotiations, NSO agreed, so the BKA acquired a modified version<sup>258</sup>. 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 that works in practice. The BKA has written a report about this modified version, which remains classified<sup>259</sup>.

## Use of Finfisher

132. In 2012 and 2013, both the German Federal Police BKA and Berlin Police LKA independently purchased FinFisher spyware (more about this spyware in chapter on the spyware industry). Also here, just 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 be compliant with German law.

## Malta

133. Several key figures from the spyware trade, have registered a business on Malta or they have obtained Maltese passports, but it seems they do not actually reside there, nor do their companies 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.

## France

### Victims in France

134. In the summer of 2021, the Pegasus Project revealed several cases of attempted hacks by the Pegasus spyware in France<sup>260</sup>. This leaked dataset included the telephone number of President Emmanuel Macron, as well as the phone numbers of 14 members of his cabinet<sup>261 262</sup>. Findings of forensic analyses have confirmed that the telephones of several ministers were infected with the Pegasus spyware<sup>263</sup>.

### Spyware companies in France

---

<sup>254</sup>[https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung\\_node.html](https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html)

<sup>255</sup>[https://www.gesetze-im-internet.de/stpo/\\_100b.html](https://www.gesetze-im-internet.de/stpo/_100b.html)

<sup>256</sup>[https://www.gesetze-im-internet.de/stpo/\\_100a.html](https://www.gesetze-im-internet.de/stpo/_100a.html)

<sup>257</sup><https://www.tagesschau.de/investigativ/ndr-wdr/spaech-software-pegasus-deutschland-101.html>

<sup>258</sup><https://www.tagesschau.de/investigativ/ndr-wdr/spaech-software-pegasus-smartphone-103.html>

<sup>259</sup> <https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-pruefbericht-zur-pegasus-software/>

<sup>260</sup> The Guardian. [Pegasus spyware found on journalists' phones, French intelligence confirms](#).

<sup>261</sup> The Guardian. [Spyware 'found on phones of five French cabinet members'](#).

<sup>262</sup> Euractiv. [France's Macron targeted in project Pegasus spyware case](#).

<sup>263</sup> The Guardian. [Spyware 'found on phones of five French cabinet members'](#).

135. France is also home to the spyware industry. Nexa technologies, part of Tal Dilian's Intellexa Alliance, is a French cyber defence and intelligence company, established in 2000<sup>264</sup>. Nexa Technologies is run by former managers of Amesys. Amesys was founded in 1979<sup>265</sup> and is known for the sale of a program called Cerebro, capable of tracking electronic communications of its victims, like email addresses and phone numbers<sup>266</sup>.

## Ireland

136. Ireland has become the Member State where some of the main spyware companies involved in scandals have registered, 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 are headquartered in Ireland, and registered at a law firm in the town of Balbriggan. It is remarkable that the application to incorporate Thalestris Limited in Ireland was submitted in November 2019 by a company formation specialist, only 12 days after the criminal investigation into Dilian and his company WiSpear by the Cypriot authorities was publicly revealed. Tal Dilian himself, CEO of Intellexa, does not appear on Irish company documents, but his reportedly second wife Sara Hamou is named as director of both Thalestris and Intellexa<sup>267</sup>.

## Luxemburg

137. Luxemburg hosts nine entities directly related to NSO Group, as was revealed by Amnesty International in June 2021<sup>268</sup>. The fact that Foreign Minister Jean Asselborn was initially only aware of two NSO entities based in the country<sup>269</sup>, and that the names of the nine companies (such as Triangle Holdings SA, Square 2 SARL, and Q Cyber Technologies SARL) do not immediately reveal the connection with NSO Group, show how opaque business structures in Luxemburg allow companies to operate completely out of the public view.

## Italy

138. So far, there have not been any reports on possible purchase of spyware by the Italian authorities. Apart from former Prime Minister and Commission President Romano Prodi, who was spied upon with Pegasus by the Moroccan secret services, no high-level cases of spying have been reported<sup>270</sup>. 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.

---

<sup>264</sup> Bloomberg. [Nexa Technologies Inc.](#)

<sup>265</sup> PitchBook. [Amesys.](#)

<sup>266</sup> Le Monde. [Vente de matériel de cybersurveillance à l'Égypte : la société Nexa Technologies mise en examen](#)

<sup>267</sup> <https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-inside-the-predators-irish-lair/>

<sup>268</sup> <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>

<sup>269</sup> <https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e>

<sup>270</sup> <https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/>

## Austria

139. In response to written questions by the National Council of Austria (the lower house), former Minister of Interior Karl Nehammer stated that Austria has not been a client of NSO<sup>271</sup>. 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.

## Estonia

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 30 million dollars deal for the surveillance software<sup>272</sup>.

## Lithuania

141. Anatoly Hurgin, a Russian-Israeli citizen, former Israeli military engineer and co-developer of Pegasus together with NSO, reportedly owns a company in Lithuania, called UAB 'Communication technologies', in the area of 'connection and telecommunication services'<sup>273</sup>. He also acquired a Maltese golden passport in 2015<sup>274</sup>.

## Bulgaria

142. In Bulgaria, export controls and export licenses for products that are categorized as 'dual-use' as outline 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 Destruction<sup>275</sup>. The current minister of Economy and Industry is Nikola Stoyanov<sup>276</sup>. Up until today, the Bulgarian authorities deny having granted export licenses to NSO Group<sup>277</sup>. 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<sup>278 279 280</sup>. These two claims are contradictory.

### *I.G. EU Institutions*

#### **Targeting of the European Commission**

---

<sup>271</sup> Responses by former Minister of Interior Karl Nehammer to Member of National Council Nikolaus Scherak, 22 September 2021, Reference 2021-0.580.421

<sup>272</sup> The New York Times. [Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia](#)

<sup>273</sup> [https://rekvizitai.vz.lt/en/company/communication\\_technologies/anatoly\\_hurgin\\_direktorius/](https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/)

<sup>274</sup> <https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429>

<sup>275</sup> Republic of Bulgaria. Ministry of Economy and Industry. [Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction](#).

<sup>276</sup> Council of Ministers of the Republic of Bulgaria.

<sup>277</sup> POLITICO. [Pegasus makers face EU grilling. Here's what to ask them.](#)

<sup>278</sup> Amnesty International. [Novalpina Capital's response to NGO coalition's open letter](#) (18 February 2019).

<sup>279</sup> Access Now. [Is NSO Group's infamous Pegasus spyware being traded through the EU?](#)

<sup>280</sup> <https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/>

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'<sup>281</sup>. 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 compromised<sup>282</sup>. On 11 April 2022, Reuters reported that Didier Reynders, Commissioner for Justice, and at least four Commission staff had been targeted with Pegasus software in November 2021<sup>283</sup>.
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 Jourová<sup>284</sup>, 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'<sup>285</sup>.
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 former Greek Commissioner and representatives in the Council**

147. On 6 November, Greek newspaper Documento published an extensive list of people who have allegedly been found to have traces of Predator on their devices, including Dimitris Avramopoulos, European Commissioner from 2014-2019 and Néa Dimokratía politician<sup>286</sup>. It is not clear whether he was targeted while he was member of the College, and who was behind, but considering the long list of targeted people, including

---

<sup>281</sup> Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022

<sup>282</sup> 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

<sup>283</sup> <https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/>

<sup>284</sup> <https://pro.politico.eu/news/148627>

<sup>285</sup> Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022,

<sup>286</sup> Documento, edition 6 November 2022.

many politicians from both Néa Dimokratía and opposition, the most plausible hypothesis is that the orders came from the entourage of the Prime Minister.

148. 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.

## II. The Spyware industry

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 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 they can be easily circumvented as Member States seek to get a competitive advantage with deliberate lax national implementation, and enforcement by the European Commission is 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<sup>287 288</sup>. Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.
150. In many cases, the nickname ‘mercenary spyware’ seems to be accurate. The sector does not have very high ethical standards, 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 Russia, when it became known that its spyware had been used on anti-Putin activists. However, in October 2022 there are signs that Cellebrite is still being used by Putin<sup>289</sup>. It is a lucrative, booming and shady market, attracting a lot of cowboys. Still, they 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 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.

---

<sup>287</sup> Makarios Drousiotis. *State Mafia*. Chapter 6. Published 2022.

<sup>288</sup> Haaretz. [Cyprus, Cyberspies and the Dark Side of Israeli Intel](#).

<sup>289</sup> <https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000>

## 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 well<sup>290</sup>. 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.

## Telecom networks

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)<sup>291</sup>. 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.<sup>292</sup>.

## NSO Group

153. Pegasus spyware is produced by NSO Group. NSO Group was founded in 2010 by Shalev Hulio, Omri Lavie and Niv Karmi, developing technology to help licensed government agencies and law-enforcement agencies to detect and prevent terrorism and crime<sup>293</sup>. Pegasus spyware is the best known product of NSO Group. It was brought onto the global market in 2011<sup>294 295</sup>.

## Corporate structure, transparency and due diligence

154. On 25 January 2010, NSO Group launched its first company in Israel. This company was registered under the name of NSO Group Technologies Limited. 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 trademark<sup>296</sup>.

## Export Controls

---

<sup>290</sup> Ot van Daalen, intervention in PEGA 27 October 2022;

EDRi Paper: Breaking encryption will doom our freedoms and rights <https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-Encryption.pdf>

<https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu>

<sup>291</sup> <https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7> was first adopted as, up to and including 5G.

<sup>292</sup> <https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/>

<sup>293</sup> NSO Group. [About us.](#)

<sup>294</sup> NYTimes. [The Battle for the World's Most Powerful Cyberweapon.](#)

<sup>295</sup> Hulio S., NSO Never Engaged in Illegal Mass Surveillance, The Wall Street Journal, 24 February 2022

<sup>296</sup> Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

155. Since the Pegasus spyware is qualified as a dual-use technology, it thus needs to receive an export license. NSO Group companies obtain their export licenses in Israel, Bulgaria and Cyprus<sup>297</sup>. Most of these licenses are granted by the Israeli authorities<sup>298</sup>. 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, 2007<sup>299</sup>. The Ministry of Defence's (MOD) Defence Export Control Agency (DECA) is responsible for the issuance of marketing and export licenses<sup>300</sup>. 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 Certificate<sup>301</sup>. 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.

### **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 NSO Group's business, eventually leaving the investors to the decision to strip the private equity firm of its control<sup>302</sup>. 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 NSO Group's activities and their compliance with the US blacklisting. The BRG inquiries of May 2022 were obstructed by NSO Group's management team<sup>303</sup>. A BRG executive stated that cooperation with NSO Group has become '*virtually non-existent*' due to NSO Group's pressure for continued sales to countries with controversial human rights records<sup>304</sup>. 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 BRG<sup>305</sup>. The Luxembourg court has dismissed these demands and BRG remains in charge of the fund controlling NSO Group<sup>306</sup>.

### **Black Cube**

157. Black Cube is an Israeli private intelligence agency comprised of former employees of Mossad, the Israeli military and Israeli intelligence services<sup>307</sup>. Their own company website dubs them as a 'creative intelligence service' finding 'tailored solutions to complex business and litigation challenges'<sup>308</sup>. Black Cube have been involved in a

---

<sup>297</sup> Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure. P. 62.

<sup>298</sup> Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

<sup>299</sup> European Parliamentary Research Service. Europe's PegasusGate. Countering spyware abuse.

<sup>300</sup> Amnesty International. Novalpina Capital's reply to NGO coalition letter (15 April 2019) and Citizen Lab letter (06 March 2019)

<sup>301</sup> European Parliamentary Research Service. Europe's PegasusGate. Countering spyware abuse.

<sup>302</sup> Financial Times. Private equity owner of spyware group NSO stripped of control of €1bn fund.

<sup>303</sup> Financial Times. NSO Group keeping owners 'in the dark', manager says.

<sup>304</sup> The New Yorker. How democracies spy on their citizens.

<sup>305</sup> Letter to Mr Jeroen Lenaers and his Vice Chairs.

<sup>306</sup> Luxembourg Times. Top five stories you may have missed.

<sup>307</sup> The New Yorker, <https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators>, 7 October 2019.

<sup>308</sup> <https://www.blackcube.com/>

number of public hacking controversies including in the US and Romania<sup>309</sup>. More particularly, the heads of Black Cube admitted spying on the former chief prosecutor of Romania's National Anti-Corruption Directorate Laura Kovesi<sup>310</sup>. Kovesi 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 job<sup>311</sup>.

## **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'<sup>312</sup>. 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

## **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 Ltd<sup>313</sup>. 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 networks<sup>314</sup>. Public scandals relating to these products triggered the move of Intellexa's main business activities from Cyprus to Greece.

## **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.

## **Poltrex**

---

<sup>309</sup> The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

<sup>310</sup> Balkan Insight. [Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case.](#)

<sup>311</sup> Haaretz. [Black Cube CEO Suspected of Running Crime Organisation. Revealed: The Romania Interrogation.](#)

<sup>312</sup> Tal Dilian. [About.](#)

<sup>313</sup> Open Corporates. Passitora Ltd. <https://opencorporates.com/companies/cy/HE318328>

<sup>314</sup> Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

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 ltd<sup>315</sup> 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 WiSpear<sup>316</sup>.

## **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 NSO Group<sup>317</sup>. Former investor in NSO Group Isaac Zack became the largest shareholder of Candiru. The company sells spyware for the hacking of computers and servers<sup>318</sup>. 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 dollar<sup>319</sup>.

## **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, 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 devices<sup>320</sup>. In over just two days in June 2022, the company probed networks in almost every country in the world<sup>321</sup>. 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.'<sup>322</sup>.

## **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

---

<sup>315</sup> Philenews. [FILE: The state insulted Avni and Dilian.](#)

<sup>316</sup> CyprusMail. [Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.](#)

<sup>317</sup> Haaretz. ['We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers](#)

<sup>318</sup> Haaretz. [Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.](#)

<sup>319</sup> CitizenLab. [Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.](#)

<sup>320</sup> <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

<sup>321</sup> <https://euobserver.com/digital/155849>

<sup>322</sup> <http://www.tykelab.it/wp/about/>

photos<sup>323</sup>. 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 Kazakhstan<sup>324</sup>, and it was also found in Romania<sup>325</sup>.

### **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)<sup>326</sup>, 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.’<sup>327</sup>. DSIRF evidently sells to non-state actors.

### **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 world<sup>328</sup>, including 11 EU Member States<sup>329</sup> and 13 ‘not-free’ countries<sup>330</sup>.

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

167. Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and individual citizens’ rights. 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. Member States 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. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing EU law<sup>331</sup>. This is not because there are legal constraints, but rather because it is a political choice. The

---

<sup>323</sup> <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

<sup>324</sup> <https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/>

<sup>325</sup> <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

<sup>326</sup> DSIRF is an abbreviation for “Decision Supporting Information Research and Forensic”

<sup>327</sup> <https://dsirf.eu/about/>

<sup>328</sup> <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/> -

<https://wikileaks.org/spyfiles4/customers.html>

<sup>329</sup> Belgium, Czech Republic, Estonia, Germany, Hungary, Italy, Netherlands, Romania, Slovakia, Slovenia, Spain

<sup>330</sup> Angola, Bahrain, Bangladesh, Egypt, Ethiopia, Gabon, Jordan, Kazakhstan, Myanmar, Oman, Qatar, Saudi Arabia, Turkey

<sup>331</sup> [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3994918](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918)

Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this stance becomes very problematic. Subsidiarity 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.

## **European Commission**

168. The European Commission, in its response to the spyware scandal, has so far limited itself to writing letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. However, it would seem that this timid admonition by the Commission will not be 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.
169. Unlike the US, the Commission has so far not undertaken an analysis of the situation nor an assessment of the companies that are active in the European market. There is no obvious legal objection against conducting such an analysis.
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 is weak. 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 report<sup>332</sup> 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. Without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.

## **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 cynical that the European Parliament does not

---

<sup>332</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223>

have the full powers to investigate, when some of its own members are victims of illegal surveillance.

## **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 Parliament<sup>333</sup>. 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.
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.
174. Even if illegal or criminal behaviour was ultimately to be proven, members of national governments cannot be impeached or made to resign from their EU jobs. This means that persons who are guilty of such acts may well continue with impunity to sit on EU bodies and take decisions affecting all European citizens.

## **Europol**

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 this, despite questions by Members on Europol's role in investigating spyware in the EU. It has not been mentioned since.
176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned. 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 State<sup>334</sup>, but so far it has been reluctant to make 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.

---

<sup>333</sup> Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

<sup>334</sup> 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.

178. On 28 September 2022, PEGA wrote a letter to Europol<sup>335</sup>, urging it to make use of its new powers under Article 6 of the Europol Regulation<sup>336</sup>. In a letter of reply dated 13 October 2022<sup>337</sup>, 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)*. *One of the five Member States has meanwhile confirmed to Europol the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust*’. It is not known which countries the letter refers to, nor whether the aforementioned criminal inquiry by one Member State concerns the abuse of spyware by EU Member State governments or by third countries.
179. The EU turns out to be quite powerless against potential criminal activity by national authorities, even if it affects the EU.
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.’<sup>338</sup>.

### European judiciary

181. The Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) play an important role in defending democracy, the rule of law and fundamental rights. However, they can only act upon a complaint or pre-judicial question. Proceedings are very lengthy and offer little concrete remedy in individual cases. Over the years, the courts have created a vast body of relevant case law, for example establishing standards for surveillance. However, these courts have no means to ensure that their ruling are enforced. So far, one complaint about the illegitimate use of spyware has been submitted to the ECtHR<sup>339</sup>. However, the road to the Strasbourg or Luxembourg courts is often long, costly, and cumbersome, as all options for national judicial proceedings must first be exhausted. This is especially the case if national prosecutors or judges fail or refuse to take a case, the bar for passing the admissibility test is high.

### 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, this may have an

---

<sup>335</sup> [https://twitter.com/EP\\_PegaInquiry/status/1576855144574377984](https://twitter.com/EP_PegaInquiry/status/1576855144574377984)

<sup>336</sup> “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.”

<sup>337</sup> File no 1260379.

<sup>338</sup> <https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ>

<sup>339</sup> Appeal by Koukakis to the European Court of Human Rights, 27 July 2022.

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.

## EXPLANATORY STATEMENT

### Europe's Watergate

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

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

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

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

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

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

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

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

The European Council and the national governments are practising omertà. There has not been any official response to the scandal by the European Council. Member State governments have largely declined the invitation to cooperate with the PEGA committee. Some governments downright refused to cooperate, others were friendly and polite but did not really share meaningful information. Even a simple questionnaire sent to all Member States about the details of their national legal framework for the use of spyware, has hardly received any substantial answers. Literally on the eve of the publication of this draft report, the PEGA committee received a joint reply from the Member States via the Council, also without any substance.

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

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

### **Europe's business**

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

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

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

The sales side of the trade in spyware is opaque and elusive, but lucrative and booming. Company structures are conveniently, if not deliberately, complex to hide from sight undesirable activities and connections, including with EU governments. On paper the sector is regulated, but in practice it manages to circumvent many rules, not least because spyware is a product that may serve as political currency in international relations. Spyware companies are established in several countries, but many have been set up by former Israeli army and intelligence officers. Most vendors claim they sell only to state actors, although backstage,

some also sell to non-state actors. It is virtually impossible to get any information about those customers, or about the contractual terms and compliance.

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

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

### **Spyware as part of a system**

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

completely exposed and defenceless against an all-powerful government, it also means all vital checks and balances of a democratic society have been disabled.

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

## **Secrecy**

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

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

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

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

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

## **Next steps**

At a time when European values are under attack from an external aggressor, it is all the more important to bolster our democratic rule of law against attacks from the inside. The findings of the PEGA inquiry are shocking and they should alarm every European citizen. It is evident that the trade in, and use of spyware should be strictly regulated. The PEGA committee will

make a series of recommendations to that effect. However, there should equally be initiatives for institutional and political reforms enabling the EU to actually enforce and uphold those rules and standards, even when they are violated by Member States themselves. The EU has to rapidly develop its defence lines against attacks on democracy from within.