European Parliament
2019-2024

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

8.11.2022

DRAFT REPORT

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

Rapporteur: Sophie in ‘t Veld

Obtenu pour vous par
Got for you by
agence europe

Contents

Obtenu pour vous par
Got for you by
agence europe

Introduction

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

Obtenu pour vous par
Got for you by
agence europe

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.

Obtenu pour vous par
Got for you by
agence europe

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.

Obtenu pour vous par
Got for you by
agence europe

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.

Obtenu pour vous par
Got for you by
agence europe

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.

Obtenu pour vous par
Got for you by
agence europe

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 Szydlo, and former Foreign Minister Witold Waszczykowski, attended dinner at the home of then Israeli Prime Minister Benjamin Netanyahu.[1] 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".[2] 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 Orban and Netanyahu.[3] Despite initial denials, in January 2022 PiS leader Jaroslaw Kaczynski confirmed the purchase of spyware by the Polish government.[4] [5] [6]

[1] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html , *29 January 2022.*
[2] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html , *29 January 2022.*
[3] Financieele Dagblad, 'De wereld deze week: het beste uit de internationale pers.' *7 January, 2022.*
[4] Financieele Dagblad, 'Liberalen Europarlement eisen onderzoek naar spionagesoftware', *12 January 2022.*
[5] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/ , *7 January 2022.*
[6] Financial Times, https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e , *8 February 2022.*

Obtenu pour vous par
Got for you by
agence europe

4. By 2018, rumours were already circulating about Pegasus, and subsequently it was discovered that the earliest case of its use dates back to March 2018.[7] The CEO and owner of Cross Media PR agency, Andrzej Dlugosz, was the first victim. It was discovered that he was hacked at least 61 times by November 2019.[8] TVN24 journalist Robert Zielinski also began reporting about the use of Pegasus in Poland in September 2018. Subsequently, the Ombudsman requested more information from the authorities, but the effort was in vain. At that time, the government continued to deny purchasing the spyware.

5. Former Chief of the Polish Supreme Audit Office (NIK) and current independent Senator Krzysztof Kwiatkowski provided crucial testimony regarding the purchase of Pegasus to the Senate Extraordinary Committee on Cases of Surveillance Using the Pegasus System in January 2022.**[9]** Having been released from the secrecy requirement associated with his position, Kwiatkowski provided the committee with invoices discovered by the NIK regarding the purchase of Pegasus.[10] Kwiatkowski further testified that the NIK had discovered accounts from the National Bank of Poland certifying the transfer in a 2018 investigation.[11] [12] The invoices show that the spyware was purchased for the Polish Central Anti-Corruption Bureau (CBA) from NSO Group.

6. Matic Sp. z o.o., an IT and Defence Systems company based in Warsaw, was used as a proxy company through which the CBA carried out this purchase.[13] The sole shareholder of Matic is the company 2CH and Ewa Chabros-Chromińska owns 60% of the shares in 2CH.[14] Both Ewa and her brother, Jerzy Chabros, who served as an official of Matic between 2010-2016 as well as 2CH for a time, have multiple files under their names at the Institute of National Remembrance.[15] The Institute conducts research into crimes committed against the Polish State during the communist period.[16] According to their records, Ewa Chabros-Chromińska and Jerzy Chabros served in the former Citizen's Militia (MO) in the Polish People's Republic as well as the former Secret Police of the Polish People's Republic (SB).[17]

7. Matic became a joint-stock company immediately after the purchase of Pegasus in November 2017 and operates with a license from the Ministry of Internal Affairs for trading in

[7] European Parliament Mission Report on the Mission to Poland of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Spyware at pg. 3.
[8] European Parliament Mission Report on the Mission to Poland of the Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Spyware at pg. 3.
[9] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1 , 18 January 2022.
[10] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1 , 18 January 2022.
[11] The Wire, https://thewire.in/world/poland-audit-office-invoice-pegasus-purchase-reopen-investigation , *4 January 2022.*
[12] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1 , 18 January 2022.
[13] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.
[14] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.
[15] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.
[16] https://ipn.gov.pl/en/about-the-institute
[17] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.

Obtenu pour vous par
Got for you by
agence europe

technologies with the security services, police, and in the arms trade according to *Wyborcza*.[18] The company is also in possession of a special licensing certificate from the Internal Security Agency, with the latest one issued in 2019, that will allow it to keep certain confidential information secret until the end of the decade.[19]

8. Adam Chrominski holds the most important role as the President of the management board of 2CH. Formerly, he was the President of both Matic Sp. z o. o. and Matic SA, but is now serving only as an official representative of Matic SA. The Ministry of Internal Affairs issued their licenses and permission in his name.[20] Chrominski has also been linked closely with Ewa Chabros-Chrominska. She shares his last name and has owned shares in a Warsaw villa with Chrominski for decades.[21]

9. The purchase of Pegasus was not financed through the regular budget of the CBA, but through the "Justice fund", meant for victims of crime.[22] [23] [24] [25] The original regulations of this fund do not allow it to be used for financing operations of the special services.[26] However, a motion to change the financial plan of the Justice Fund was presented to the Sejm Public Finance Committee by Michał Woś, the Deputy Minister of Justice. [27] [28] Woś is a close associate of Minister of Justice Zbigniew Ziobro, who also holds the position of Prosecutor General.[29] The MPs approved this change, but reported subsequently that they had no idea that it was about purchasing Pegasus for the CBA, given that 'during the committee meeting, not a single word was said about it'.[30]

10. Woś also applied to the Ministry of Finance for consent to re-allocate the PLN 25 million that was spent on Pegasus from the Justice Fund to 'other activities' aimed at 'combating the effects of crime'.[31] The Deputy Minister then signed for the transfers from the Justice Fund

[18] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.
[19] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.
[20] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.
[21] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html , 17 January 2022.
[22] The Guardian, 'More Polish opposition figures found to have been targeted by Pegasus spyware', *17 February, 2022.*
[23] The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', *24 January 2022.*
[24] 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 at pg. 26.
[25] Gazeta Wyborcza, https://www.rp.pl/polityka/art19250101-gazeta-wyborcza-jak-kupowano-pegasusa-dla-cba , *3 January 2022.*
[26] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1 , 18 January 2022.
[27] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html , 4 January 2022.
[28] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27966080,jak-ziobro-kupowal-pegasusa-dla-cba.html , *3 January 2022.*
[29] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html , 4 January 2022.
[30] https://polishnews.co.uk/pegasus-reports-of-surveillance-and-backstage-of-the-purchase-themis-judges-association-on-a-possible-breach-of-the-law-appeal-to-appoint-a-commission-of-inquiry/ , *4 January 2022.*
[31] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27966080,jak-ziobro-kupowal-pegasusa-dla-cba.html , *3 January 2022.*

Obtenu pour vous par
Got for you by
agence europe

to the CBA.[32] [33] However, upon being asked in January 2022, Woś initially denied having any knowledge of the Pegasus tool itself, let alone its purchase by the state,[34] [35] but he has since confirmed the purchase.[36] It is unclear how the running costs for the use of Pegasus have been funded.

11. It has been reported that in total, NSO Group has sold to 14 countries in Europe thus far. However, NSO has also conceded that it has revoked the licenses of two such countries.[37] It is highly possible that Poland was included as one of these two countries in light of their breach of the NSO terms of use; however, this has not been confirmed. It is not known if the Polish authorities have purchased another brand of spyware.

Legal Framework

12. 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.[38] The Tribunal concluded by issuing a judgement containing specific recommendations and an 18-month timeline within which legislative changes were to be implemented.[39] 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.[40] 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.

13. The scope for surveillance and so-called operational control was vastly expanded, weakening or removing safeguards and oversight provisions. Broadening statutes in this systematic and targeted manner under domestic law keeps the legal basis for surveillance firmly in contravention with EU law, the 2014 ruling of the Polish Constitutional Court and the fundamental rights of the Polish citizens. In this way, unlawful surveillance is thus legalised. The law of the ruler has replaced the rule of law.

14. In its opinion on the 2016 Police Act, the Venice Commission unequivocally states that '...procedural safeguards and material conditions set in the Police Act for implementing secret

[32] ONET**,** https://wiadomosci.onet.pl/kraj/wiceminister-michal-wos-nie-wiem-co-to-jest-pegasus/e9fbrvh , *3 January 2022.*
[33] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html , *4 January 2022.*
[34] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html , *4 January 2022.*
[35] DW, https://www.dw.com/en/who-hacked-polands-opposition/a-60332256 , *1 May 2022*.
[36] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html , *4 January 2022.*
[37] Discussion with NSO Group, Mission of the Committee of Inquiry to Investigate the use of Pegasus and Equivalent Surveillance Spyware to Israel, July 2022.
[38] Venice Commission Report June 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e .
[39] https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani
[40] 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 .

Obtenu pour vous par
Got for you by
agence europe

surveillance are still insufficient to prevent its excessive use and unjustified interference with the privacy of individuals'.[41] Moreover, the lack of specificity regarding oversight, guarantees against abuse, and the categories of persons and crimes that could be targeted also violate the judgements of the European Court of Human Rights (ECtHR).[42] In particular, in the judgement of the *Roman Zakharov v. Russia* case in 2015, the Court examined the need for clarity regarding the use of spyware. It was held that in relation to secret surveillance of citizens there is a necessity for strict criteria, proper judicial oversight, immediate destruction of irrelevant data, judicial scrutiny over urgency procedures and a requirement for the notification of victims.[43] In summary, the Court stated that much of the provisions in Russian domestic law do not provide 'adequate and effective guarantees against arbitrariness and the risk of abuse'.[44] Moreover, the Court explicitly stated that it would be 'contrary to the rule of law' if discretion regarding secret surveillance was concentrated entirely with the executive of the judiciary.[45] The 2016 Police Act that remains in effect in Poland in no way reflects this ruling of the Court. In fact, its provisions are in direct contravention with much of the judgement.

15. The ECtHR has also been unequivocal in its stance on the necessity test, meaning that the act of surveillance must be of sufficient importance to necessitate such an invasion of privacy. Its judgement in the *Klass and others v. Germany* case in 1978 outlined this point clearly, and held that no matter the system of surveillance, the Court must be satisfied that there exists 'adequate and effective guarantees against abuse'.[46] The blatant corruption and carefully orchestrated destruction of checks and balances in Poland show the evident defiance of the Courts by the ruling party. Despite all of this, the PiS led government insist that existing provisions are sufficient, and they are operating strictly inside the law.[47]

Anti-Terrorism Law 2016

16. 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.[48] The prosecutor general is responsible for ordering the destruction of non-

[41] Opinion No. 839/2016 on the act of 15 January 2016 amending the Police Act and certain other acts, adopted by the Venice Commission at its 107th plenary session, 10-11 June 2016
[42] 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.
[43] Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015 39.
[44] Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015 39.
2008.
[45] Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015 39 at pp.229 and 230. See also Venice Commission Report June 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e at pg. 11.
[46] Klass and others v. Germany, 6 September 1978, § 50, Series A no. 28. 40.
[47] TVP Info, https://www.tvp.info/57607147/zaryn-ws-senatora-brejzy-falszywe-sa-sugestie-ze-sluzby-nielegalnie-wykorzystuja-kontrole-operacyjna-do-gry-politycznej , *23 December 2021.*
[48] Act of 10 June 2016 on Anti-terrorism Operations, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf .

Obtenu pour vous par
Got for you by
agence europe

relevant materials and, Zbigniew Ziobro, the PiS Minister of Justice, currently holds that office.[49] [50]

Code of Criminal Procedure

17. 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.[51] 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.[52]

Telecommunications Law of 16 July 2004

18. 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.[53] 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. [54] [55]

19. The abovementioned amendment to the Code of Criminal Procedure to allow "fruit of the poisonous tree" has had a significant impact on the importance of the telecommunications operators and the data those companies store. In Poland, the biggest telecommunications providers have to go so far as to have a dedicated team that responds to the requesting for wiretapping from the authorities, but usually do not have much insight on the content of wiretapping or more details connected with a specific case. [56] [57] [58] [59]

[49] Act of 10 June 2016 on Anti-terrorism Operations, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf .
[50] EDRi, https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/ , *29 June 2016.*
[51] 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
[52] 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
[53] Telecommunications Act of 16 July 2004 https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004 .
[54] 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 .
[55] Helsinki Foundation for Human Rights, 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].
[56] https://www.europarl.europa.eu/doceo/document/PEGA-CR-736647_EN.pdf
[57] 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.*
[58] 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
[59] https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf at pg. 16-17.

Obtenu pour vous par
Got for you by
agence europe

Ex-ante Scrutiny

20. 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.[60] 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.[61] The information is often merely a summary, sometimes excluding even the most basic details regarding the target (name, profession, the crime of which he/she is suspected), and the surveillance methods to be used.

21. The choice of surveillance method makes a big difference. Contrary to conventional wiretapping, which allows for the real time monitoring of communications, spyware allows for files (documents, images, etc.), messages and metadata about communications to be retrieved retroactively. This means that a judicial decision on and entry date and limited duration of the surveillance operation, has no meaning in the case of spyware.

22. Yet, if a judge rejects an application, they are required to give a reasoned justification for such a decision and it can be subject to appeal.[62] Crucially, in urgent cases, the prosecutor can initially authorise the use of interception methods without the approval of a judge, provided the court subsequently grants authorisation within five days.[63] This is a significant and deliberate loophole in the legal framework.

23. Requests for authorisation of surveillance by the main agencies, i.e. the CBA, the police (Policja KGP), and the intelligence services (Agencja Bezpieczenstwa Wewenetrznego, Centralne Biuro Antykorupcyjne, Straz Graniczna, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Sluzba Kontrwywiadu Wojskowego, Sluzba Ochrony Panstwa, Biuro Nadzoru Wewnętrznego MSWiA, and the recently added Inspektorat Służby Więziennej) are submitted almost exclusively to the Regional court in Warsaw (Sad Okręgowy), where the majority of these agencies are established.

24. Several dozen surveillance applications are submitted every day, stretching the capacity of the court to conduct an in-depth examination of each request.[64] The system which randomly allocates cases to the judges of the courts is technically still in operation in Poland, but it is only functional during business hours. However, given that the Court which authorises surveillance functions on a 24-hour basis, there is ample opportunity for the system to be

[60] 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 .
[61] 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 .
[62] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef
[63] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef
[64] Testimony of Ewa Wroszek, Country Specific Hearing on Poland, Meeting of the Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, 15 September 2022.

Obtenu pour vous par
Got for you by
agence europe

circumvented. By submitting an application at the weekend or outside of normal business hours, the case will be automatically assigned to the judge who is on call.[65] The information regarding who is on call at any given time is known to the secret services, who are then essentially able to select a "friendly judge" to whom they can submit their surveillance requests.[66] Additionally, random allocation can also be by-passed by IT personnel who have access to the system and could assign surveillance authorisations to "friendly judges".[67]

Ex-post Scrutiny

25. 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. Jaroslaw Krajewski as Deputy Chairman.[68] The government parties have the absolute majority in the committee.[69] Moreover, the government majority in the Sejm rejected calls for a parliamentary investigation into the allegations of the illegitimate use of spyware. [70] [71] [72] [73] [74] 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.[75]

26. Scrutiny and remedies offered by other independent bodies have also been severely weakened. The Supreme Audit Office has effective powers of oversight; however, its members and staff are subject to constant obstruction, harassment and intimidation, which is severely affecting its operational capacity.[76] [77] The Sejm has so far failed to appoint ten of the nineteen members

[65] Testimony of Ewa Wroszek, Country Specific Hearing on Poland, Meeting of the Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, 15 September 2022.
[66] Testimony of Ewa Wroszek, Country Specific Hearing on Poland, Meeting of the Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, 15 September 2022.
[67] Testimony of Ewa Wroszek, Country Specific Hearing on Poland, Meeting of the Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, 15 September 2022.
[68] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS
[69] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS
[70] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422 *17 January 2022.*
[71] 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 at pg. 27.
[72] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, *23 December 2021*.
[73] The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', *24 January 2022.*
[74] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/ , 18 January 2022.
[75] 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 at pg. 27, footnote 220.
[76] Reuters, https://www.reuters.com/article/poland-pegasus-idUSL8N2UF596 , *4 February 2022.*
[77] Discussion with Supreme Audit Office, Mission of the Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, September 2022.

Obtenu pour vous par
Got for you by
agence europe

of the NIK council.[78] [79]The required vetting of council members carried out by the special services, headed by Minister Kaminski, is very slow.[80]

27. When a violation of the law is discovered by the NIK, they have the power to submit notification to the Prosecutor's office.[81] However, it is up to the office of the Prosecutor to initiate a case on the basis of that violation. In situations where the Prosecutor does not take action, there is little that can be done by NIK. When a reported violation concerns operation of the Prosecutor's office itself, a vicious circle of non-accountability is created. In addition, all cases notified by NIK to office of the Prosecutor must be reported to the Prosecutor General, who is also the Minister of Justice, heading the very ministry that purchased the spyware in the first place.
28. The Sejm consistently refuses to grant discharge to NIK each year, and when Marian Banās, the head of NIK, uses his statutory speaking time in Sejm, MPs of the governing parties leave the room.[82]

29. The current Ombudsman Marcin Wiącek was appointed in 2021 when the Sejm and Senate agreed on a non-partisan compromise candidate after a long tug of war.[83] So far, he has not intervened in cases relating to abuse of spyware. Notably, regarding the case of Senator Brejza, Wiącek argues that the Ombudsman should not get involved in the early stages of a case. Despite this, both the former and current Ombudsmen have been monitoring the situation and asserting a certain amount of pressure on the need to create an independent oversight body to provide democratic control on the operations of the secret services.[84]

Reporting

30. 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).[85] 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.[86]

[78] https://www.nik.gov.pl/en/about-us/the-council-of-nik/
[79] Discussion with Supreme Audit Office staff, Mission of the Committee of Inquiry to Investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, September 2022.
[80] Discussion with Supreme Audit Office staff, Mission of the Committee of Inquiry to Investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, September 2022.
[81] Act of 23 December 1994 on the Supreme Audit Office https://www.nik.gov.pl/en/about-us/legal-regulations/act-on-the-supreme-audit-office.html at Article 63.
[82] Discussion with Supreme Audit Office staff, Mission of the Committee of Inquiry to Investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, September 2022.
[83] Euractiv, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/ , *22 July 2021*.
[84] Europe's PegasusGate - European Parliament Research Service, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf , at pg. 22.
[85] 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 .
[86] HFHR Report at pg.4.

Obtenu pour vous par
Got for you by
agence europe

Redress

31. So far, the Polish prosecutor has 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 able to appeal to the Courts. In late September 2022, the Warsaw District Court (Mokotów) ordered the prosecutor to begin an investigation.[87]

32. It is critical to note that Wrzosek was only able to initiate this appeal in the Courts as a result of obtaining an official refusal from the office of the Prosecutor. In many other instances, the Prosecutor will drag out their investigation in order to avoid ever having to issue an official response, as they are aware that if they do so they will be exposed to the appeals process in the Courts.

33. Citizens who have been targeted can of course bring a civil case before court, but the burden of proof is on the plaintiff and it is virtually impossible to prove the illegitimate use of spyware without the cooperation of the authorities. The lack of implementation of the duty to notify in Poland, as outline in the *Klass* judgement, means many persons may never know they have been targeted.

34. NIK have submitted official notification to the Prosecutor's office regarding a violation of the law concerning the use of resources of the Justice Fund to purchase Pegasus in 2017. However, given the current institutional and political environment, there is no expectation that the office of the Prosecutor will take action on such a case.

35. Currently, the cases *Pietrzak v. Poland* and *Bychawska-Siniarska and others v. Poland* are before the ECtHR challenging the lack of transparency, oversight, notification and remedies when it comes to surveillance in Poland. Significantly, the Court decided to conduct a rare hearing for these cases, which took place on 27 September 2022. The cases were taken by five citizens[88] who submitted complaints to the ECtHR in September 2017 and February 2018 respectively. Eleven entities submitted their amicus curiae briefs in this case, including European Criminal Bar Association [89], the Polish Ombudsman, and the UN Special Rapporteur on counter-terrorism and human rights[90].

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

[87] Wyborcza, https://wyborcza.pl/7,75398,28963729,pegasus-w-telefonie-ewy-wrzosek-prokuratura-odmowila-sad-kaze.html , *28 September 2022.*

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

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

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

Obtenu pour vous par
Got for you by
agence europe

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

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

39. It is worthy of note that Poland has not yet implemented the **EU Whistle-blowers Directive**. It did not meet the December 2021 deadline after its initial draft legislation failed. A second draft was published in April 2022 but there has been no further progress and the proposed legislation contains significantly weaker provisions. In January 2022, the Commission opened an infringement procedure against Poland for failing to fully implement the Directive. In July 2022, the Commission sent a reasoned opinion to Poland.[91] No further development has been communicated since.

Public Scrutiny

40. 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.

[91] https://ec.europa.eu/commission/presscorner/detail/en/inf_22_3768

Obtenu pour vous par
Got for you by
agence europe

Political Control

41. 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.[92] 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.[93]

42. Minister of Justice Ziobro, is also the Prosecutor General. Concerns over this combination of offices have been raised frequently in recent years. Mr. Ziobro plays a very central role in the entire chain described above. Mr. Ziobro equally has declined to meet with or co-operate with the PEGA committee.

43. It has been established that the CBA is a government controlled body [94] [95] despite its title and its mandate which was established under the *Act of 9 June 2006 on the Central Anti-Corruption Bureau*[96], and which states in Article 1.1 that "[t]he Central Anti-Corruption Bureau ... is established as a special service to combat corruption in public and economic life, particularly in public and local government institutions as well as to fight against activities detrimental to the economic interest of the State" [97]. In the 2022 Annual Rule of Law Report, the Commission finds that "The independence of main anti-corruption institutions remains an issue, considering in particular the subordination of the Central Anti-Corruption Bureau to the executive and the Minister of Justice also being the Prosecutor-General".

44. The state capture of the judiciary has been well established and confirmed by a wide range of instances, including the European Commission and the European Court of Justice.

45. Not only has the legal and institutional context been created to enable near unlimited surveillance with spyware, virtually all parts of the process are also firmly controlled by the government parties. As a result, none of the safeguards that exist on paper, have any meaning in practice.

The Targets

46. 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

[92] Reuters, https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117 *17 November 2015.*
[93] EU Observer, https://euobserver.com/rule-of-law/156063 , *15 September 2022.*
[94] Politico, https://www.politico.eu/article/marian-banas-poland-takes-on-law-and-justice-government/, *13 May 2021.*
[95] 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 at pg.16. "The independence of main anti-corruption institutions remains an issue, considering in particular the subordination of the Central Anti-Corruption Bureau to the executive and the Minister of Justice also being the Prosecutor-General"
[96] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf
[97] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf, at Art. 1.1.

Obtenu pour vous par
Got for you by
agence europe

in 2019.[98] 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.[99] 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.

47. Previously, Citizen Lab had detected a number of infections in Poland in late 2017; however, they were not able to identify the victims at that time.[100]

48. The Polish Senate launched a Commission of Investigation into these attacks in early 2022 despite its lack of inquisitorial competences[101], however they have been opposed at every turn by the ruling party in the Sejm (lower house) [102], which refuses to co-operate or conduct its own investigation.[103] [104] [105] [106] [107]

49. The use of spyware and efforts to control citizens must be seen in close connection with the election system. Several targets of Pegasus were somehow connected to elections: Senator Krzysztof Brejza (opposition leader), Roman Giertych (lawyer of Donald Tusk), Ewa Wrzosek (prosecutor investigating the postal voting for the presidential elections), Supreme Audit Office (NIK) (published reports on the postal vote for the presidential elections), and Michael Kolodziejczak (founding a new opposition party, competing for the same electorate as the governing parties).

50. At the same time, the National Electoral Commission has been politicised by virtue of the fact that is comprised of judges from the very courts that the ruling party have essentially taken over. Furthermore, the District Court in Warsaw responsible for the registration of new political parties[108] has been filled with government-loyal "neo-judges". In view of this, concerns exist whether the 2023 parliamentary elections will be truly free and fair.

---

[98] 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.*

[99] Financieele Dagblad, 'De wereld deze week: het beste uit de internationale pers.' *7 January, 2022.*

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

[101] 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 at pg. 27, footnote 220.

[102] Bloomberg, https://www.bloomberg.com/news/articles/2022-01-03/polish-government-urged-to-probe-spyware-use-as-scandal-grows?leadSource=uverify%20wall#xj4y7vzkg , *3 January 2022.*

[103] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422 *17 January 2022.*

[104] 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 at pg. 27.

[105] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, *23 December 2021.*

[106] The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', *24 January 2022.*

[107] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/ , 18 January 2022.

[108] Act of 27 June 1997 about Political Parties, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970980604/U/D19970604Lj.pdf, at Art. 11.

Obtenu pour vous par
Got for you by
agence europe

Senator Krzysztof Brejza

51. Senator Krzysztof Brejza was serving as campaign leader of the opposition party Civic Platform when he was the victim of hacking with spyware.[109] 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.[110]

52. As a direct result of the hacking of Brejza's phone, text messages were allegedly stolen, doctored and subsequently aired on the state-controlled television network (TVP) [111] [112] during the 2019 elections in an alleged orchestrated smear campaign[113]. This has caused Senator Brejza to call in to question the legitimacy of the 2019 election, which was narrowly won by the ruling PiS party.[114]

53. Although the PiS Government admits to obtaining Pegasus, it vehemently denies allegations that it was used for political purposes.[115] Kaczynski has neither confirmed nor denied targeting Brejza, but has alleged that the Senator was linked to "suspected crimes", something Brejza strongly denies.[116] By the implication that Brejza was linked to criminal activity, it created circumstances through which the Polish government would have used Pegasus spyware for one of the grounds that the NSO group deem 'legitimate' when considering whether to sell their software to a government, namely the investigation of serious criminal activity[117].

54. At the time however, a criminal investigation into Senator Brejza's father, Ryszard Brejza, was initiated. While serving as the mayor of Inowroclaw, a city in central Poland, Brejza Sr. was called in for questioning in relation to alleged mishandling of public funds and failing to carry out his duties.[118] This questioning occurred directly after Brejza Jr. initiated legal proceedings against Kaczynski for slander. Both Krzysztof and Ryszard Brejza have asserted that the charges against Brejza Sr. were a retaliation for the lawsuit.

55. Ryszard Brejza himself received 10 text messages between July and August 2019 which Amnesty International's security lab deemed suspicious and matched the hallmarks of

[109] 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.*
[110] The Guardian, 'More Polish opposition figures found to have been targeted by Pegasus spyware', *17 February, 2022.*
[111] 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 at pg. 20 - 23.
[112] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, *23 December 2021.*
[113] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, *23 December 2021.*
[114] Financieele Dagblad, https://fd.nl/politiek/1426857/liberalen-europarlement-eisen-onderzoek-naar-spionagesoftware , *12 January 2022.*
[115] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/ , *7 January 2022.*
[116] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/ , *7 January 2022.*
[117] BBC, https://www.bbc.com/news/technology-57881364 , *19 July 2021.*
[118] AP, https://apnews.com/article/technology-business-software-hacking-spyware-8cc528ba7d46a61b378adf1ede9dd00f , 10 January 2022.

Obtenu pour vous par
Got for you by
agence europe

Pegasus.[119] [120] The former assistant of Senator Brejza, Magdalena Losko, also received four suspicious text messages in April 2019 while running Senator Brejza's European Parliament Campaign, which, according to Amnesty International forensic examiners, were technically consistent with NSO group's spyware Pegasus.[121]

Roman Giertych

56. 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 Peoples 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.[122]

57. As with the case of Senator Brejza, the government would neither confirm nor deny whether they were responsible for these attacks. It was reported by the Associated Press that a motion seeking the arrest of Giertych was filed by a prosecutor regarding an alleged financial crimes investigation, which Giertych vehemently denies, just a matter of hours before state security spokesperson Stanislaw Zaryn responded to questions from the AP regarding the hacking of Giertych's phone. Zaryn refused to comment on the possible connection between these incidents. In a similar incident, Giertych's home was raided and searched by CBA officials in 2020. [123]

58. Additionally during this time in 2019, Giertych was representing Gerald Birgfellner, an Austrian developer. Birgfellner had been involved in investigating a property for PiS leader Kaczynski, with whom he has family ties, when the deal went sour. Following the release of recorded conversations between the two, a political scandal erupted for Kaczynski who then quickly ended all interest in the property. Birgfellner alleges that he was never paid for his services and so engaged Giertych. [124] [125] Minister for Justice and Prosecutor General Zbigniew Ziobro also commented in 2021 that he was seeking to bring charges against Giertych "with the suspicion of committing criminal crimes".[126]

---

[119] The Guardian, 'More Polish opposition figures found to have been targeted by Pegasus spyware', *17 February, 2022.*
[120] Le Monde, https://www.lemonde.fr/pixels/article/2022/07/18/affaire-pegasus-un-an-apres-le-crepuscule-de-nso-group_6135168_4408996.html, *18 July 2022.*
[121] The Guardian, 'More Polish opposition figures found to have been targeted by Pegasus spyware', *17 February, 2022.*
[122] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e *21 December 2021.*
[123] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e *21 December 2021.*
[124] AP, https://apnews.com/article/elections-international-news-jaroslaw-kaczynski-european-parliament-poland-bed5ffc814e649f4bb4d10f82628b4c2 , *16 February 2019.*
[125] TVP World, https://tvpworld.com/41262080/ruling-party-leader-im-no-dictator , *11 February 2019.*
[126] TVP Info, https://www.tvp.info/57607147/zaryn-ws-senatora-brejzy-falszywe-sa-sugestie-ze-sluzby-nielegalnie-wykorzystuja-kontrole-operacyjna-do-gry-politycznej , *23 December 2021.*

Obtenu pour vous par
Got for you by
agence europe

Ewa Wrzosek

59. 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.[127] 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.[128] 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. [129] [130]

Other Possible Targets

Supreme Audit Office

60. 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[131] 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.[132]

61. The media have previously reported that Banās has links with a fraudulent VAT scheme during that was allegedly run by his close associate out of the finance ministry during tenure as Minister of Finance. It was additionally reported at that time that Banās owned a building in Krakow that was being run as a "by-the-hour" hotel by a person with criminal ties.[133]

62. The timing of the attacks is particularly relevant given the nature of the investigation NIK was conducting. The spokesperson for NIK, confirmed that it was investigating the cancellation of the Presidential elections in 2020. The results of this probe saw the Prime Minister, members of his government, and a Justice Ministry Fund served with notifications of crimes. This had led to further allegations of the PiS government using Pegasus for political reasons, which they deny as "fake news".[134]

63. Previously, the Sejm has considered stripping Banas of the immunity from prosecution that he enjoys as head of NIK following a motion filed by Minister of Justice Zbigniew Ziobro in

[127] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e *21 December 2021.*
[128] 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 at pg. 16.
[129] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e *21 December 2021.*
[130] The Guardian, https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony , *24 January 2022.*
[131] https://www.nik.gov.pl/en/about-us/
[132] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/ , 18 January 2022.
[133] Politico, https://www.politico.eu/article/marian-banas-poland-takes-on-law-and-justice-government/ , *13 May 2021.*
[134] Notes from Poland, https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/ , *7 February 2022.*

Obtenu pour vous par
Got for you by
agence europe

his role as Prosecutor General.[135] Security spokesperson Zaryn reported that prosecutors were seeking to charge Banas in relation to a number of financial crimes including false tax declarations.[136]

64. In July 2021, Banas' son Jakub was arrested and detained by the CBA in relation to a number of alleged financial crimes linked with his father and NIK.[137] In May 2021, Jakub was subject to a raid by the CBA. Banas believes this repeated targeting of his family is politically motivated in order to force his resignation.[138]

65. It is clear that the government is making every effort to obstruct the scrutiny carried out by NIK of the purchase and use of Pegasus.

PiS Associates

66. 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.[139] [140] 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.

67. In addition, former PiS Member of Parliament Mariusz Antoni Kaminski and former PiS Minister of the State Treasury Dawid Jackiewicz were allegedly targeted with Pegasus by the government.[141] Mariusz A. Kaminski was cast out of the PiS party as a result of being embroiled in a scandal at the same time as Hofman, however Jackiewicz remains a member of the ruling party despite his sudden step back from his ministerial role.[142]

68. A similar smear campaign was also conducted against the former President of the Employers of the Republic of Poland, Mr. Andrzej Malinowski, in February 2018 by the ruling party. He testified in front of a special sitting of a Senate Committee in April 2022 regarding the hacking of his phone with Pegasus in order to collect the information for this public takedown.[143] He outlined that messages were taken from his WhatsApp and SMS through Pegasus and were strategically used to spread online hate against him. This attack was retaliation for disagreeing with the ruling party and demanding alternative economic policies.

---

[135] TVP World, https://tvpworld.com/55013822/prosecutors-office-calls-for-stripping-supreme-audit-office-head-of-his-immunity *23 July 2021.*
[136] Notes from Poland, https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/ , *7 February 2022.*
[137] Polish News, https://polishnews.co.uk/jakub-banas-son-of-marian-banas-the-head-of-the-supreme-audit-office-was-arrested-by-the-central-anticorruption-bureau/ , *23 July 2021.*
[138] Politico, https://www.politico.eu/article/marian-banas-poland-takes-on-law-and-justice-government/ , *13 May 2021.*
[139] https://wyborcza.pl/7,173236,28015977,polish-state-surveilled-nearly-50-targets-with-pegasus-spyware.html?disableRedirects=true
[140] Rzeczpospolita, https://www.rp.pl/polityka/art4805251-hofman-usuniety-z-pis-decyzja-w-sprawie-hofmana , *11 October 2014.*
[141] https://wiadomosci.onet.pl/kraj/pegasus-oto-kolejne-osoby-ktore-mialy-byc-inwigilowane-przez-sluzby-pis/yvt6tym
[142] https://nextvame.com/dawid-jackiewicz-is-back-jaroslaw-kaczynski-confirms-the-reports/
[143] https://www.senat.gov.pl/prace/komisje-senackie/przebieg,9668,1.html

Obtenu pour vous par
Got for you by
agence europe

Connection with Smear Campaigns

69. 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.

Obtenu pour vous par
Got for you by
agence europe

I.B. Hungary

70. 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[144] that over 300 Hungarians have fallen victim to Pegasus, including political activists, journalists, lawyers, entrepreneurs and a former government minister. [145]

71. The use of Pegasus in Hungary appears to be part of a calculated and strategic destruction of media freedom and freedom of expression by the government. [146] The Fidesz government has utilised this spyware in order to introduce a regime of harassment, blackmail, threats and pressure against independent journalists and media moguls. As a result, there now remains only a handful of independent Hungarian media outlets and in 2021, Orban became the first EU leader to be placed on the Enemies of Press Freedom list by Reporters without Borders (RSF).[147] Although the government consistently fall back on reasons of 'national security'[148], claims that the victims are a threat to national security are preposterous.

Purchase of Pegasus

72. The Hungarian Ministry of the Interior bought Pegasus from NSO Group in 2017 shortly after Orban met with Polish Prime Minister Mateusz Morawiecki and former Israeli Prime Minister Benjamin Netanyahu.[149] [150] 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 Kosa, acknowledged the purchase of Pegasus by the Fidesz government.[151] Kosa still insisted however that the spyware has never been used against Hungarian citizens.[152]

73. President of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), Attila Péterfalvi, has continuously asserted that all use of Pegasus was for national security purposes, which falls within the exclusive competence of national governments.[153] [154] The ruling party refuses to confirm or deny that the government targeted certain politically motivated victims.[155]

---

[144] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 February 2022.*
[145] DW, 'Pegasus scandal: In Hungary, journalists sue state over spyware', *29 January 2022.*
[146] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*

[147] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[148] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 February 2022.*
[149] Financieele Dagblad, De wereld deze week: het beste uit de internationale pers. *7 January, 2022.*
[150] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[151] DW, Hungary admits to using NSO Group's Pegasus spyware', *4 November 2021.*
[152] DW, Hungary admits to using NSO Group's Pegasus spyware', *4 November 2021*
[153] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 February 2022.*
[154] Netzpolitik, https://netzpolitik.org/2022/pegasus-scandal-in-hungary-not-surprising-but-still-shameful/ , *10 February 2022.*
[155] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0 , *4 November 2021.*

Obtenu pour vous par
Got for you by
agence europe

74. In response to calls from the opposition, the Fidesz government held two special committee hearings, including one in the Committee on Defence and Law Enforcement, however they subsequently classified the findings of those hearings until 2050.[156]

Legal Framework

75. The legal instruments governing spyware in Hungary are some of the weakest such provisions in Europe.[157] [158] 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[159] despite the government's insistence that they have acted legally in all instances and are completely compliant with the law.[160] [161] The *Act CXXV of 1995 on National Security Services* (hereinafter the Act) is currently governing the use of spyware in Hungary[162] 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.[163] The requirement to notify victims was unequivocally established in the case of *Klass and others v. Germany*[164] in the ECtHR and the Hungarian government have failed to implement this ruling it in the same manner as Poland and many other countries within the EU.

76. Moreover, its vague provisions do not clearly outline the types of crimes or criteria that warrant surveillance. These deficiencies concern some of the most basic provisions regarding spyware required under EU law, along with proper oversight and scrutiny to prevent abuse and effective avenues for redress, which are also nowhere to be found in the text of the Act.

77. With respect to the practical element of conducting surveillance through the use of spyware, telecommunications companies have a significant role to play. There are countless instances of victims being infected through links sent via SMS, and the wealth of data that telecommunications companies have access to is a goldmine for those wishing to conduct surveillance. In the case of Hungary, the situation has become increasingly more dangerous as the Hungarian government recently bought Vodafone Hungary.[165] This will grant the government easy and direct access to the data of more than 3 million customers.[166]

---

[156] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0 , *4 November 2021.*
[157] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[158] DW, 'Pegasus scandal: In Hungary, journalists sue state over spyware', *29 January 2022.*
[159] 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.
[160] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0 , *4 November 2021.*
[161] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 February 2022.*
[162] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf .
[163] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Section 58.
[164] Klass and others v. Germany, 6 September 1978, § 50, Series A no. 28. 40.
[165] Reuters, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/ , *22 August 2022.*
[166] Reuters, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/ , *22 August 2022.*

Obtenu pour vous par
Got for you by
agence europe

Additionally, resulting from this purchase the state will have an access point to the decades-old global messaging system known as SS7.[167] This system allows mobile operators to connect users around the world. The Hungarian state will also be able to lease such and access point further, as was the case for Rayzone.[168]

78. There is a legal framework for the legal interception of calls in Hungary, which is contained in *Act CXXV of 1995 on National Security Services*. Specifically, section 56 states that 'based on an external permission, national security services ... may secretly intercept and record the content of communications conducted through an electronic communications network or device using an electronic communications service, or through an information system.'[169]

79. In addition to this relative free rein, the Counter Terrorism Centre agency of Hungary can employ almost any known ways of surveillance. For the unit to exercise these powers they do not need any prior legal authorisation. In this case, a ministerial approval is sufficient.[170] [171]

Ex-ante Scrutiny

80. 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-Capital Regional Court in some specific cases.[172] [173] No appeal can be made against these decisions and there is virtually no oversight of the process.[174] [175]

81. Despite the gravity of such a decision, when she is not available Minister of Justice Judit Varga delegates responsibility for the authorisation of spyware use against citizens to the Secretary of State of the Ministry of Justice, a position currently held by Robert Repassy.[176] [177] This was confirmed by Repassy himself in a response he authored to written questions on the issue.[178] It is widely reported that Varga regularly passed off the responsibility to Repassy's predecessor Pal Volner, who was forced to resign from the role in December 2021 as a result of a major corruption scandal.[179] [180] It was widely reported that he accepted millions

[167] The Guardian, https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands , *16 December 2020*.
[168]
[169] [169] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Section 56.
[170] [170] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf .
[171] https://clfr.globalnetworkinitiative.org/country/hungary/
[172] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Sections 56-58.
[173] Europe's PegasusGate: Countering Spyware Abuse - EPRS Report, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf , July 2022 at pg. 20.
[174] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Sections 57 and 58.
[175] European Commission Rule of Law Report 2022, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf , at pg. 26.
[176] https://telex.hu/belfold/2021/12/10/repassy-robert-igazsagugyi-allamtitkar-varga-judit-igazsagugyi-miniszterium
[177] Europe's PegasusGate: Countering Spyware Abuse - EPRS Report, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf , July 2022 at pg. 20.
[178] https://telex.hu/belfold/2022/01/27/varga-judithoz-kerulhetett-vissza-a-titkos-megfigyelesek-engedelyezese
[179] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye
[180] https://hungarytoday.hu/444-key-figure-in-volner-corruption-case-gyorgy-schadl-judge-fired-judiciary-obh/

Obtenu pour vous par
Got for you by
agence europe

of Hungarian forint in bribes from a number of high profile stakeholders in return for favourable decisions and appointments to key positions by Volner in his capacity as Secretary of State.[181]

82. While the Interior Minister Sandor Pinter insists that this authorisation procedure through the Minister or the Courts is always followed without exception[182], the weak legal provisions of the Act also make it possible for the directors-general of the SNSS to grant interim permission for the conducting of surveillance without consent until such time as official permission can be granted. This essentially allows the SNSS to operate as they see fit so long as they claim that the delay in obtaining permission would harm their operation. In such a case, the unauthorised surveillance can continue without oversight until permission is granted or denied.[183]

83. This loophole is particularly troubling given that it would be very possible in theory to cite urgency and complete the necessary surveillance within a matter of hours, theoretically never needing to officially obtain permission at all. This type of hacking leaves many questions unanswered regarding the processing and retention of data gathered during such a period.

84. The legal limit of a maximum of 90 days for surveillance imposed in the Act is in itself a contradiction and only presents to give the appearance of legal oversight, given that the Act subsequently allows for a further 90-day extension upon a simple request from the director-general to the permitting officer.[184] Moreover, contrary to conventional wiretapping, the use of spyware allows to access files (i.a. document, images) created in the past, as well as the metadata of past communications. That renders a date of entry and a time limit rather meaningless. Information dating from before the start of the authorised surveillance, can be retrieved without limit.

85. In addition, the NAIH are theoretically supposed to oversee all surveillance by the secret services. The body was created as part of a reforms to scale down the office of the Ombudsman and to take over the work of the abolished office of the Parliamentary Commissioner for Data Protection .[185] However, given that the head of the NAIH is appointed by the Prime Minister, all pretence of independent oversight is eradicated.[186] The ECtHR has ruled on the matter in October 2022 in a case of *Hüttl v. Hungary*[187] taken by HCLU lawyer Tivadar Hüttl when after he was hacked with Pegasus spyware, his complaint to the National Security Committee was blocked, and an investigation was denied.[188] The Court clearly stated in their judgement that the NAIH, though entitled to investigate the actions of the secret services, were completely incapable of conducting independent oversight of the use of mercenary spyware. The Court held that the NAIH lacked the necessary competence to do so, given that the secret services are entitled to deny access to certain documents on the basis of

[181] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye
[182] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0 , *4 November 2021.*
[183] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Section 59.
[184] Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Section 58.
[185] HGV, https://hvg.hu/itthon/20111117_Peterfalvi_palyaja_adatvedelem , *21 November 2011.*
[186] https://hclu.hu/en/pegasus-whats-new
[187] https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-219501%22]}
[188] https://tasz.hu/cikkek/valoszinusithetoen-lehallgattak-pert-nyert-strasbourgban-a-tasz-ugyvedje

Obtenu pour vous par
Got for you by
agence europe

secrecy.[189] In such an instance, it would fall to the Minister responsible for the secret services to conduct an audit, which could not be deemed independent oversight in any way.[190]

Ex-post Scrutiny

86. 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.

87. An NAIH investigation was launched following allegations of at least ten lawyers, the President of the Hungarian Bar Association, and at least five journalists being targeted.[191] The resulting report was published on 31 January 2022 and concluded that the use of Pegasus was strictly for reasons of national security. Furthermore, according President of the NAIH Attila Péterfalvi, the investigation did not uncover any illegal activity or anything inconsistent with the terms of sale of NSO Group.[192] That is remarkable in view of the fact that it is widely assumed that Hungary is one of the two countries that have been struck off the list of fourteen EU countries to which NSO sells its products.

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

89. Considering that authorisation power rests within the Justice Ministry, and the Fidesz backed Prosecutor General, Peter Polt, was re-elected in 2019 for a further nine years (having already served for a combined period of 15 years over two different terms up to that point), it is very difficult to conclude that all of this governmental oversight is anything other than a charade for appearances sake.

90. There is no support to be found within the Hungarian anti-corruption framework in response to this given that the Ministry of the Interior, who initially purchased Pegasus from NSO Group, is responsible for the coordination of all anti-corruption policy and oversight.[193]

Redress

91. 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

[189] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere
[190] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere
[191] European Commission Rule of Law Report 2022, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf at pg. 26.
[192] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 February 2022.*
[193] European Commission Rule of Law Report 2022, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf at pg. 10.

Obtenu pour vous par
Got for you by
agence europe

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.[194]

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

93. There is also a long-standing battle over the last two years regarding access to information. In order to request access files containing all data gathered on any one citizen, you must know the exact name of the file to which your request relates, which is almost impossible information to acquire. Having been inevitably rejected by the Supreme Court in their requests, the HCLU sought a ruling from the Constitutional Court declaring this practice, and the ruling of the Curia unconstitutional. However, in 2021, the Constitutional Court rejected the HCLU's motion.

94. In addition to its lawsuits before the courts, the HCLU has also pursued other avenues to access their data. An administrative procedure was initiated and accepted under the Classified Data Act and the Data Protection Act. However, there will be a yearlong review by the Constitution Protection Office in each individual case before any results will be known.[195] Additionally, the spyware attacks have been reported to the Commissioner for Fundamental Rights (Ombudsman). The Constitutional Court has stipulated that the responsibility lies with the Ombudsman to investigate abuses by the secret services, but it is very likely that the procedure will only result in the Ombudsman pushing responsibility on to the government controlled NAIH.[196]

95. In another attempt to achieve some transparency, the HCLU has requested access to the data being collected and processed resulting from the hacking of the six victims in a process that is conducted outside the courts system. However, the entitlement to this information only exists as long as providing the data to the subjects does not interfere with national security.[197] This creates another pretext for the Hungarian authorities to once again fall back on national security reasons.[198] So far, the Constitution Protection Office has rejected 270 Freedom of Information (FOI) requests submitted by the HCLU between 2018 and May of 2022.[199]

96. The ECtHR has already ruled on the situation in Hungary in the case of *Szabo and Vissy v. Hungary* in 2016 and held in its judgement that there was insufficient judicial supervision of the authorisation of covert surveillance in Hungary. It was also outlined by the Court that there was a gap in the legal framework regarding effective remedy. The ruling parties have yet to act on this judgement however, and as a result, they are under heightened supervision by the Council of Europe.

[194] The Guardian, https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state , *28 January 2022.*
[195] https://hclu.hu/en/pegasus-case-hungarian-procedures
[196] https://hclu.hu/en/pegasus-whats-new
[197] https://hclu.hu/en/pegasus-case-hungarian-procedures
[198] https://hclu.hu/en/pegasus-whats-new
[199] https://hclu.hu/en/pegasus-whats-new

Obtenu pour vous par
Got for you by
agence europe

Political Control

97. The political control over the use of surveillance in Hungary is complete and total. The Orban 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.

98. The Minister of the Interior was responsible for the purchase of Pegasus spyware in the first instance, and the Minister for Justice remains in charge of authorising its use. However, the ruling party classified results of the investigations into the use of spyware that were conducted by special committee hearings until 2050. It can only be deduced from this that the findings were not favourable to Fidesz. The legislative framework of Hungary regarding the surveillance of its citizens has been repeatedly found lacking, however the ruling party make no moves to alter it as it suits their own agenda.

99. The Prime Minister selects the head of the NAIH, the body supposedly responsible for the independent oversight of Pegasus use by the secret services. Given that he is a political appointee, the illusion of independence is destroyed. Hungary and the Fidesz government are no strangers to these types of political appointments. In fact, over the years of Orban's rule, Hungary has become the *de facto* European capital of cronyism.[200] Fidesz has systematically placed party loyalists into leading roles in bodies such as Constitutional Court, the Supreme Court, the Court of Auditors, the prosecution service, the National Bank of Hungary and the National Election Committee.[201] This ensures that any institution created with the intent of conducting oversight of the executive branch cannot carry out its role in an independent manner.[202]

The Targets

100. It has been very clear that the government's actions were politically motivated from the moment that the spyware scandal broke in Hungary. It was reported that the phone numbers of over 300 persons were included in the findings of the Pegasus Project. [203] Among those were at least five journalists, ten lawyers and an opposition politician as well as activists and high profile business owners.[204] 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

[200] 'Hungary. Lobbying, State Capture and Crony Capitalism', J. Martin and M. Ligeti [2017] pg. 177-193 at pg. 178 in *Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries*, (A. Bitonti and P. Harris eds., Springer 2017).
[201] 'Hungary. Lobbying, State Capture and Crony Capitalism', J. Martin and M. Ligeti [2017] pg. 177-193 at pg. 178 in *Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries*, (A. Bitonti and P. Harris eds., Springer 2017).
[202] 'Hungary. Lobbying, State Capture and Crony Capitalism', J. Martin and M. Ligeti [2017] pg. 177-193 at pg. 178 in *Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries*, (A. Bitonti and P. Harris eds., Springer 2017).
[203] Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ , *19 July 2021*.
[204] 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*.

Obtenu pour vous par
Got for you by
agence europe

methodical and systematic actions and attitude of Orban'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

101. 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.

102. It was confirmed by Amnesty International that Panyi's phone was consistently hacked in 2019 over a period of seven months.[205] These attacks were pointed and often occurring at a time when Panyi had requested the government to provide a comment on issues. A specific and concerning example of this occurred on 3 April 2019. Panyi contacted the government requesting a comment on the article he wrote detailing the move of a Russian bank to the Hungarian capital which was a high-profile story given that there were questions about whether or not the bank was in fact a front for Russian intelligence services.[206] Amnesty International confirmed that Panyi's phone was hacked the following day, and additionally verified that there were eleven other such instances of hacking in the immediate aftermath of a request for comment from Orban's administration.[207] That equates to over half of Panyi's requests resulting in being targeted within that seven month period.[208] This is an abhorrent violation of media freedom.

103. The ruling party have feigned ignorance with regard to the targeting of Panyi and will not confirm nor deny that they were responsible. However, the government has previously attacked Panyi publicly, with Orban's spokesperson alleging that he was a fanatical political activist as well as accusing him of Orbanophobia and Hungarophobia.[209] This is a blatant attempt to discredit Panyi and paint both his sources and himself as the 'enemy' through the government's own state-controlled media.

Zoltan Varga

104. As CEO and Chairman of Central Media Group, Zoltan Varga is the owner of Hungary's largest remaining independent news site 24.hu. After the Orban 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.

105. Fidesz has been conducting a smear campaign against Varga via the government-controlled media for some time in order to discredit both his personal public figure and the publication,

[205] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[206] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[207] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[208] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[209] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*

Obtenu pour vous par
Got for you by
agence europe

despite its popularity, with an audience of over 7.5 million per month.[210] [211] Varga alleges that he was both enticed and threatened to sell on different occasions, including offers for generous state advertising subsidies in return for hiring the government's choice of editorial staff.[212] Varga first suspected his phone was infected with Pegasus when he began hearing a playback of the call in while in mid-conversation. Subsequently in 2021, it was discovered by Amnesty International that Varga had indeed most likely been hacked by Pegasus, but it could not be confirmed owing to the fact that the phone had since been replaced.[213]

106. Additionally, shortly after the 2018 elections, the re-elected Orban attempted to get to Varga indirectly. Following a dinner party to discuss the government media takeover hosted by Varga in spring 2018, which included Attila Chikan, a former Fidesz Minister turned Orban critic, it was verified that all those present were recorded as being candidates for surveillance.[214] It was subsequently confirmed that one guest was hacked at the time of the party, while other phones showed traces of potential Pegasus hacks but no proof of successful infection.[215] The hacking was all but confirmed by a government affiliated acquaintance of Vargas who directly referenced the dinner party in conversation and warned against socialising with people who could be "dangerous".[216]

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

Adrien Beauduin

108. Adrien Beauduin appeared on the radar of the Orban 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.[217] 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.[218] 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.[219]

[210] Politico, https://www.politico.eu/article/viktor-orban-bent-on-muzzling-independent-press-hungarian-media-mogul-warns-index-24-hu-news-sites/ , *25 July 2020.*
[211] Politico, https://www.politico.eu/article/viktor-orban-bent-on-muzzling-independent-press-hungarian-media-mogul-warns-index-24-hu-news-sites/ , *25 July 2020.*
[212] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[213] Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ , *19 July 2021.*
[214] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[215] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[216] Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ , *19 July 2021.*
[217] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[218] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[219] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*

Obtenu pour vous par
Got for you by
agence europe

109. At the time, government representatives publically condemned so-called "pro-immigration Soros network" for orchestrating "violent demonstrations in Budapest".[220] Subsequently, traces of Pegasus were found on Beauduin's phone, but it was not possible to confirm whether there had been a successful infection.

110. Given that Beauduin was a Belgian citizen living in Hungary at that time of these incidents, the importance of the cross-border element in this case cannot be overstated. It is critical as it affects the sovereign rights of EU citizens, such as freedom of movement and the right to work. The Commission has a complaints procedure in place that any person can avail of if their Charter rights have been breached. Adrien Beauduin lodged such a complaint on 24 January 2022, however seven months later, in a letter of response dated 17 August 2022 addressed to his lawyer it was outlined that it would not be possible for the Commission to do anything as it does not have the competence. [221]

Ilona Patocs

111. Lawyer Ilona Patocs 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.[222] 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, Istvan Hatvani, had already served seven years for an assassination, which Patocs claims was a "politically motivated" conviction.[223] 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 Janos Banati.[224] This targeting in particular shows a clear disregard from the government for the privilege that exists between lawyers and their clients.

Other Targets

112. 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 Janos Ader, bodyguard to the President and close ally of Orban, 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.

113. Additionally, both the son and lawyer of one of Orban's oldest friends, Lajos Simicska, were hacked with Pegasus.[225] Simicska went from being a close friend of Orban to being an opponent. He was in the process of selling his media consortium that had fuelled much of the

[220] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests , *18 July 2021.*
[221] European Commission letter of response from Cathrin BauerBulst, Head of Unit Directorate General for Migration and Home Affairs, dated 17 August 2022.
[222] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/ , 31 March 2022.
[223] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/ , 31 March 2022.
[224] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/ , 31 March 2022.
[225] Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ , *18 July 2021.*

Obtenu pour vous par
Got for you by
agence europe

feud following Orban's electoral victory in 2018 when this relational targeting occurred.[226] Simicska himself was not target for the simple reason that he does not use a smartphone, thus rendering impossible infection through spyware such as Pegasus.[227] Ajtony Csaba Nagy, Simicska's lawyer, suspected an infection where he heard a playback of his conversation with Simicska during a phone call. Later, those suspicions were seemingly confirmed when information only discussed on those calls appeared in Hungarian media.[228] Given that the majority of news outlets in Hungary are state owned, it is likely that the government provided the information directly to the media themselves.

Spyware Companies

114. 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.[229] Their own company website dubs them as a "creative intelligence service" finding "tailored solutions to complex business and litigation challenges".[230] Black Cube have been involved in a number of public hacking controversies including in the US and Romania.[231] 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.

115. Black Cube got involved in Hungary during the 2018 elections, during which time they spied upon various NGOs and persons who had any connection to George Soros and reported back to Orban in order for him to spin their actives in a smear campaign.[232] Those targeted included lawyer and member of the leading human rights NGO Hungarian Helsinki Committee, Marta Pardavi.[233] The resulting information from the surveillance of those individuals and NGOs appeared not only in the Hungarian state-controlled media, but also in the Jerusalem Post.[234]

116. An additional connection with Hungary is Cytrox Holdings ZRT which is registered at an address in Budapest. Cytrox was originally founded in North-Macedonia and created the Predator spyware tool before it was bought by WiSpear, which is now part of the Intellexa alliance run by Tal Dilian.

[226] Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ , *18 July 2021.*
[227] Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ , *18 July 2021.*
[228] Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/ , *18 July 2021.*
[229] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators , 7 October 2019.
[230] https://www.blackcube.com/
[231] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , 18 April 2022.
[232] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/ 6 July 2018.
[233] Reuters, https://www.reuters.com/article/meta-facebook-cyber-idCNL1N2T12MC , 16 December 2021.
[234] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/ 6 July 2018.

Obtenu pour vous par
Got for you by
agence europe

I.C. Greece

117. 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 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.[235] The attempted infection with spyware was discovered during a check of Androulakis' phone by the European Parliament IT service.[236] 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,[237] 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.[238] On 5 and 6 November, the Greek media revealed a list of 33 targets, all of whom were high profile personalities.[239] 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.[240][241]

118. In August 2022, the Greek government conceded that EYP had indeed been monitoring Androulakis and Koukakis, but it denied the use of Predator spyware in these surveillance operations. In addition, other cases of surveillance by the EYP came to light during this period, such as that of journalist Stavros Malichoudis.[242][243][244] To date, the official reasons for the surveillance have not been disclosed.

119. On 8 August 2022, Prime Minister Mitsotakis issued a video message stating ambiguously that the surveillance of Androulakis was "legal" but "politically unacceptable". He made no reference to the surveillance of Koukakis, nor the alleged other cases. He also stated that he had not been aware of the surveillance, but had he known, he would not have allowed it.[245] It is noted though that the EYP is under the direct control of Prime Minister Kyriakos

[235] Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.
[236] Tagesspiegel. Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.
[237] Reuters. One more Greek lawmaker files complaint over attempted phone hacking.
[238] Efsyn. Targeting the disliked.
[239] Documento. Apocalpyse: They Watched - This Sunday in Document.
[240] Meta. Threat Report on the Surveillance-for-Hire Industry.
[241] InsideStory. Who was tracking the mobile phone of journalist Thanasis Koukakis?
[242] Solomon. Solomon's reporter Stavros Malichudis under surveillance for "national security reasons".
[243] Ekathimerini. Wiretapping case: The phone data that triggered developments.
[244] EPRS. Greece's Predatorgate. The latest chapter in Europe's spyware scandal?
[245] Reuters. Greek PM says he was unaware of phone tapping of opposition party leader.

Obtenu pour vous par
Got for you by
agence europe

Mitsotakis following a legislative amendment, passed soon after his party Néa Dimokratía came to power in 2019.[246]

120. After the revelations, Grigoris Dimitriadis, nephew of Prime Minister Mitsotakis, and the government's General Secretary responsible for the cooperation between the Greek government and the EYP, and EYP Chief Panagiotis Kontoleon, resigned.[247]

121. Both EYP and the government categorically deny that Predator has ever been purchased or used by the Greek authorities.[248] Despite the fact that the use of spyware is illegal in Greece, there does not appear to be a vigorous search for the origins of the spyware attacks.

122. 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.

123. 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.

124. With a view to the general election due in spring 2023, the situation must be urgently clarified, so as not to cast any doubt on the integrity of the elections in 2023.

Purchase

125. The government denies the purchase of Predator spyware.[249] 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

[246] Euractiv. Another Greek opposition lawmaker victim of Predator.
[247] POLITICO. PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal.
[248] EPRS. Greece's Predatorgate. The latest chapter in Europe's spyware scandal?
[249] Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.

Obtenu pour vous par
Got for you by
agence europe

hypothesis of private actors behind the Predator attacks is moreover highly implausible, as it would not explain the choice of targets.

126. 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.

127. 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.

128. The situation in Greece is of an impenetrable complexity, but there are a few persons and entities that play a key role.

Grigoris Dimitriadis

129. Mr 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.

130. The former head of the EYP, Panagiotis Kontoleon, admitted to the Greek Parliamentary Inquiry Committee his "social relationship" with Dimitriadis. Kontoleon was appointed by the Mitsotakis government, but some provisions of the law had to be adapted so as to enable his appointment.[250]

131. Dimitriadis is also closely connected in several ways to Felix Bitzios and Giannis Lavranos. The three men are personally acquainted. Dimitriadis and Lavranos are best men ("Koumbaroi")[251] and Lavranos is the godfather of Dimitriadis' second child.[252] Dimitriadis was also indirectly connected to Bitzios through business transactions with Bitzios' brother.[253]

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

133. Dimitriadis is reportedly also acquainted with Adreas Loverdos, candidate for the PASOK-KINAL leadership in 2021.

[250] Ieidiseis. SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up.
[251] TVXS. Giannis Lavranos: The koumbarias with Tsouvala and Dimitriadis.
[252] Ieidiseis. SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up.
[253] ReportersUnited. The Great Nephew and Big Brother.

Obtenu pour vous par
Got for you by
agence europe

Felix Bitzios

134. 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.[254] 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[255]. Thanks to the amendment of the Mitsotakis government, the assets of Bitzios could be released.

135. Bitzios is connected with Cyprus through his company Santinomo, registered on Cyprus, and his connection with Tal Dilian. It seems that Bitzios has been instrumental in the transfer of Intellexa to Greece.[256]

136. Felix 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.[257] What is remarkable is not just the date of the registration of the transfer - just days after the revelations of the Androulakis hack - but the fact that the transfer supposedly took place on 18 December 2020, over 19 months earlier. Bitzios thus retroactively distanced himself from his 1/3 Intellexa ownership. Nevertheless, Bitzios had been connected to Intellexa from March 2020 to June 2021 as a deputy administrator.

Giannis Lavranos

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

Intellexa

138. 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.[258] However, Intellexa companies based in Greece reportedly exported their products to Bangladesh and at least one Arab country. [259][260] For a detailed description on Intellexa see the chapter on the Spyware Industry.

[254] Lexocology. Cyprus court offers directions to bank on ambit of freezing injunction.
[255] Financial Times. Greek law change viewed as backtracking on money laundering.
[256] Inside Story. Predatorgate: The second shareholder of Intellexa SA.
[257] Inside Story. Predatorgate: The second shareholder of Intellexa SA.
[258] Inside Story. Who signs the exports of spyware from Greece and Cyprus?
[259] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[260] Inside Story. Who signs the exports of spyware from Greece and Cyprus?

Obtenu pour vous par
Got for you by
agence europe

Krikel

139. 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.[261] 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.

140. 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.[262] In 2014, the Greek government had also shown interest in the Italian spyware brand called RCS Galileo from company Hacking Team, as revealed by Wikileaks, but this software was never acquired.[263] 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 euros. Krikel administrator Stanislaw Pelczar (see below) signed on behalf of Krikel, but it seems that Lavranos was informally involved in the negotiations throughout.[264] Krikel became an important supplier of the Greek Ministry of Citizen Protection. Since 2018, it signed seven contracts with the Greek government, six of which are secret.[265]

141. Krikel company also became the local representative of Italian company RCS Lab. In June 2021, the EYP purchased a wiretapping system from RCS lab[266] through Krikel.[267] At that time, Grigoris 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 Nikos Androulakis and Thanasis Koukakis was lost, allegedly caused by a technical problem.[268] Other sources however claimed that Kontoleon ordered the destruction of files on 29 July 2022.[269]

142. Interestingly employees of Krikel have been spotted working at Ketyak, allegedly "pro bono". Ketyak has apparently been granted 40 million euros from the RRF, through a confidential tender procedure based on a secret decision of the Prime Minister.

---

[261] 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].

[262] Inside Story. Predatorgate's invisible privates.

[263] Inside Story. The timeless interest of the Greek authorities in spyware. https://insidestory.gr/article/diahroniko-endiaferon-ton-ellinikon-arhon-gia-logismika-kataskopeias

[264] Inside Story. Predatorgate's invisible privates.

[265] InsideStory. Predatorgate's invisible privates.

[266] Hellas Posts Engllish. The EYP supplier contaminates smartphones in Greece as well.

[267] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.

[268] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.

[269] Euractiv. Greek MEP spyware scandal takes new turn.

Obtenu pour vous par
Got for you by
agence europe

Involvement of Bitzios and Lavranos

143. 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.[270] 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).[271]

144. Bitzios and Pelczar have other mutual business connections as well. It emerges from the Paradise Papers that they share a company registered on Malta by the name of Baywest Business.[272] In addition, Tal Dilian, the founder of Intellexa holds a Maltese (golden) passport[273] and also has a letterbox company MNT Investments LTD in the island state.[274]

145. 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 Mr 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 Mr Koykakis. 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.

146. Yet, despite the obvious relevance of Bitzios and Lavranos testifying before the Inquiry Committee of the Greek parliament, the Néa Dimokratía majority on the committee rejected the requests of the opposition for these men to be heard.[275]

Legal Framework

147. 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

148. 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

[270] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.
[271] InsideStory. From Koukakis to Androulakis: A new twist in the Predator spyware case.
[272] International Consortium of Investigative Journalists. Offshore Leaks Database. Paradise Papers - Malta Corporate Registry.
[273] 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
[274] https://mlt.databasesets.com/company-all/company/73006 https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/
[275] Ieidiseis. SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up.

Obtenu pour vous par
Got for you by
agence europe

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.[276]

149. The number of authorised wiretaps has increased substantially over the years. From 4871 in 2015 (when Syriza came to power), to 11,680 in 2019 (when Nea Demokratia came to power) to 15,475 in 2021.[277] Currently, some 60 request have to be processed each day, until recently by a single prosecutor. Moreover, the provisions of the EYP that lift the confidentiality of citizens' communications for reasons of national security do not mention the name of the person concerned nor the reason for the lifting of confidentiality. They are limited to the telephone number and the invocation of national security.[278]

150. The judicial authorisation to monitor private communication as well as the extension and the termination of such an authorisation have to be approved by the competent Public Prosecutor. As stipulated in law 3649/2008, the competent prosecutor to lift secrecy and confidentiality is the in-house prosecutor of the EYP. A legislative amendment from 2018 had reduced the number of prosecutors required for the authorisation of a wiretap from two to one. The prosecutor in charge of the cases at hand is Vasiliki Vlachou.[279] Mrs Vlachou did not meet with the PEGA mission to Greece.

Act of Legislative Content

151. 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.[280] 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.[281] Incidentally, 2nd deputy commander of the EYP is Dionysis Melitsiotis[282], a former member of the private office of the Prime Minister, and another Deputy Director is Anastasios Mitsialis, a former Nea Demokratia official.[283]

152. In addition, the act reintroduced the two-prosecutor authorisation of monitoring requests.[284] Article 5 of law 3649/2008 on the provision for the lifting of confidentiality of communications by the EYP is supplemented with a submission for approval to the

[276] ICLG. Cybersecurity Laws and Regulation Greece 2022.
[277] Ekathimerini. Wiretapping and 'national security'.
[278] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis.
[279] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis.
[280] Efsyn. What (does not) change with the Act of Legislative Content for EYP.
[281] Kathemirini. Themistoklis Demiris: His appointment to the management of EYP was approved by a majority.
[282] Ekathimerini. National security takes center stage.
[283] Greek City Times. Greek PM appoints new security and intelligence chiefs.
[284] European Parliament. Greece's Predatorsgate: The latest chapter in Europe's spyware scandal?

Obtenu pour vous par
Got for you by
agence europe

competent Prosecutor of Appeals, and after that, approved of by the Public Prosecutor of the Court of Appeals.[285]

Ex-post scrutiny

153. 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.[286]

154. Parliamentary control is exercised by the Permanent Committee on Institution and Transparency. This committee supervises the actions of the EYP and has the power to collect documents, examine persons and invite the Director General for a hearing.[287] As mentioned above, the current committee consists of an overall majority of the government party.

155. The Hellenic Authority for Communication Security and Privacy (ADAE) ensures the protection of confidentiality of mail and all other sorts of communications.[288] The statute of ADAE grants it administrative autonomy.[289] ADAE can carry out investigations at facilities, databases, archives, technical equipment and documents of the EYP.[290]

156. 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.[291] 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.[292] 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.[293] 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 measures) and the deadlines required by the Constitution were not respected.[294][295][296] There was therefore no proper consultation process.

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

---

[285] Efsyn. What (does not) change with the Act of Legislative Content for EYP.
[286] Euractiv. Another Greek opposition lawmaker victim of Predator.
[287] Centre for European Constitutional Law. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies.
[288] ADAE. Presentation.
[289] ADAE. Regulatory framework.
[290] Centre for European Constitutional Law. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies.
[291] Constitutionalism. Contradiction of article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications.
[292] Dpa. Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data.
[293] https://www.reportersunited.gr/8646/eyp-koukakis/
[294] Hellenic Parliament. Constitution.
[295] Hellenic Parliament. Rules of Procedure of the House.
[296] Govwatch. Violation of the legislative process for amendments in law 4790/2021.

Obtenu pour vous par
Got for you by
agence europe

158. The possibilities for ex-post scrutiny are further weakened by the fact that Greece has still not fully implemented the EU Whistleblowers Directive. On 27 January 2022, the Commission launched an infringement procedure by sending a formal notice to Greece. On 15 July 2022, the Commission sent a reasoned opinion with a deadline of two months to reply. However, up to date not much progress has been recorded in the legislative procedure.[297] It is not known whether or not the Commission will refer Greece to the Court of Justice of the European Union.

Public scrutiny

159. Greece ranks lowest of all EU countries in the World Press Freedom Index 2022: 108 out of 180.[298] In 2021, journalist Giorgos Karaivaz was murdered. The murder has still not been resolved. Journalists face intimidation and SLAPPs. Grigoris Dimitriadis[299] launched Strategic Lawsuits against Public Participation (SLAPPS) against news outlets Reporters United and Efimerida ton Syntakton (EfSyn)[300] 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.[301] 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 Triantafillou reported about the spyware scandal, and they were allegedly put under surveillance.[302]

Redress

The National Transparency Authority

160. As stipulated in article 82 of Law 4622/2019, the National Transparency Authority (EAD) has the responsibility to strengthen the accountability, transparency and integrity of actions undertaken by government bodies, state bodies, administrative authorities and public organisations. In addition, the EAD ought to prevent, detect and address actions of fraud and corruption by public and private bodies. According to this law, the National Transparency Authority has taken over all responsibilities, rights and obligations from the following public bodies: The General Secretariat for the Fight against Corruption; the Body of Auditors-Inspectors of Public Administration; the Office of the Inspector General of Public Administration; the Body of Inspectors of Health and Welfare Services; the Body of Inspectors of Public Works; and the Body of Inspectors-Auditors of Transport.[303]

161. On 22 July 2022, the EAD started an inquiry into the alleged purchase of the Predator spyware by the Ministry of Citizen Protection and the EYP. The audit checked the Hellenic

[297] https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768
[298] https://rsf.org/en/index
[299] Tagesspiegel. .
[300] EUobserver. Greece accused of undermining rule of law in wiretap scandal.
[301] https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/
[302] Heinrich-Böll-Stiftung. In conditions of absolute loneliness.
[303] https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019

Obtenu pour vous par
Got for you by
agence europe

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.[304]

162. In the end, the EAD report concluded that both the EYP and the Ministry of Citizen Protection had not concluded contracts with Intellexa and other related national companies. They also had not purchased or used the Predator spyware.[305] 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 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. [306]

163. 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.[307] 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)

164. 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.

165. Normally the Predator spyware does not leave traces of infection at the telecommunications providers. However, the ADAE did find that the mobile phone of Androulakis was monitored by the EYP, and that its in-house prosecutor Vasiliki Vlachou had authorised the monitoring action and the lifting of secrecy in September 2021, coinciding with the alleged Predator attack.[308][309]

166. Following the findings of the ADAE inquiry Grigoris Dimitriadis and Panagiotis Kontoleon, resigned from their government positions.[310] Kontoleon stated that the monitoring of Androulakis was set off at the request of foreign authorities - more specifically the Intelligence agencies of Armenia and Ukraine - in light of Androulakis' partaking in the

[304] InsideStory. From Koukakis to Androulakis: A new twist in the Predator Spyware case.
[305] InsideStory. From Koukakis to Androulakis: A new twist in the Predator Spyware case.
[306] InsideStory. From Koukakis to Androulakis: A new twist in the Predator Spyware case.
[307] https://www.politico.eu/article/greek-transparency-agency-report-data-breach-migration-european-commission/
[308] Kathimerini. Surveillance hypothesis: The data that triggered the developments.
[309] European Parliament. Greece's Predatorsgate: The latest chapter in Europe's spyware scandal?
[310] POLITICO. PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal.

Obtenu pour vous par
Got for you by
agence europe

European Parliament committee on trade relations between the European Union and China.[311] Both Ukraine and Armenia have repudiated these claims.[312]

The Committee on Institutions and Transparency

167. 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.[313]

168. Although the meetings are in camera[314] neither Kontoleon nor Dimitriadis were willing to provide substantial evidence, invoking national secrecy reasons.[315] The new head of EYP Demiris denied the committee access to a report containing information on the alleged destruction of surveillance data.[316] This effectively means that the EYP refuses accountability and the Parliament cannot carry out its mandate of parliamentary oversight.

169. On 30 August, the committee summoned nine people for a closed-door hearing, including public prosecutor Vasiliki Vlachou, former Secretary General Grigoris Dimitriadis and former head of EYP Kontoleon. All of them invoked confidentiality and avoided answering questions during this committee hearing.[317]

The Parliamentary Committee of Inquiry

170. A proposal by the PASOK-KINAL party to set up a committee of inquiry into the alleged use of spyware[318] was endorsed by 142 MPs of the opposition, while the 157 Nea Demokratia MPs abstained.[319] 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.

171. 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

[311] Kathimerini. Surveillance hypothesis: The data that triggered the developments.
[312] European Parliament. Greece's Predatorsgate: The latest chapter in Europe's spyware scandal?
[313] Reuters. Greek intelligence service admits spying on journalist - sources.
[314] Ekathimerini. Transparency committee to hold closed-door meeting on phone hacking allegation.
[315] Tovima. In combat positions for eavesdropping.
[316] Tovima. In combat positions for eavesdropping.
[317] Ieidiseis. SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.
[318] Tovina. Interceptions: Committee of Inquiry to monitor Androulakis - Pasok's proposal in detail.
[319] Tovina. Parliament: The examination for the attendances from 2016 was passed - With 142 "yes".

Obtenu pour vous par
Got for you by
agence europe

information about the involvement of Bitzios and Lavranos in Krikel, claiming *i.a.* that he himself was the owner of Krikel.[320]

172. One witness, Mrs 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 5500 pages of documents, including the minutes and the deposition of Mrs 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.

173. The opposition proposed some other witnesses, such as Koukakis, Mitsotakis, Dimitriadis, Vlachou, Lavranos, and Bitzios but the committee eventually denied to invite them. On 10 October 2022, the committee finished its investigations and the different political parties all submitted their final reports.[321]

The Targets

174. 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

175. 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).[322] 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.

176. On 29 July 2022 EYP chief, Panagiotis Kontolean declared that the EYP had monitored Koukakis' phone in light of ‘national security reasons’.

177. On 1 June 2020, the EYP submitted a first request to lift the confidentiality of the telephone number of Koukakis for two months, until 1 August 2020. EYP submitted a request for an

[320] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.
[321] Ieidiseis. SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.
[322] Inside Story. Who was tracking the mobile phone of journalist Thanasis Koukakis.

Obtenu pour vous par
Got for you by
agence europe

extension by an additional two months[323], i.e. until 1 October 2020. The Prosecutor of the Court of Appeals - Vasiliki Vlachou - has approved all these provisions under the invocation of national security.[324][325]

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

179. On 10 March 2021, the ADAE reported to the Prosecutor of the EYP on the possibility of notifying Koukakis about the surveillance of his mobile phone. However, on 31 March, the Greek government submitted Amendment 826/145 depriving the ADAE of the ability to notify citizens of the lifting of the confidentiality of communications with retroactive effect.[326][327] The president of ADAE Christos Rammos and two other members of the ADAE have argued against this amendment, pointing out in an OpEd that the amendment violates the right to respect for private and family life of the European Convention on Human Rights (ECHR) and the protection of confidentiality of communications as guaranteed in the Constitution.[328]

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

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

182. The investigation by the National Transparency Authority (EAD) on 21 July 2022 into the Athens offices of Intellexa, the vendor of Predator spyware, was limited and superficial, despite the fact that vital information on the Predator attacks - a criminal offence - could

[323] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis.
[324] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis.
[325] Inside Story. Who was watching journalist Thanasis Koukakis' cell phone?
[326] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis.
[327] Inside Story. Who was watching journalist Thanasis Koukakis' cell phone?
[328] Constitutionalism. Contradiction of article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications.
[329] Inside Story. Who was watching journalist Thanasis Koukakis' cell phone?
[330] European Parliament. Hearing September 8, 2022.
[331] Inside Story. Who was watching journalist Thanasis Koukakis' cell phone?
[332] Avgi. Thanasis Koukakis / Filed a lawsuit for the Predator – Who and why was watching him.

Obtenu pour vous par
Got for you by
agence europe

have been found. No servers, IT hardware or administration were seized and secured. The verification of the financial administration was limited to the year 2020.[333] The Cyprus and Ireland subsidiaries of Intellexa were not investigated at all.[334] The investigations did not include information on the bank accounts of Intellexa and subsidiaries.[335] Koukakis appealed to the European Court of Human Rights on 27 July 2022.[336]

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

Nikos Androulakis

184. 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.[339] 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.[340]

185. In September 2021, Androulakis 'announced his candidacy in the race for party leadership.[341] According to the ADAE inquiry, the mobile phone of Androulakis was at that time monitored by the EYP through the telecommunications providers.[342] EYP Prosecutor Vasiliki Vlachou approved the lifting of secrecy of Androulakis 'phone on "national security" grounds. The approval coincided with both the Predator targeting and Androulakis 'candidacy.

186. When Mr Androulakis was elected party leader in December 2021, the "official" EYP monitoring was terminated abruptly[343], despite the fact that the two-month authorisation for his surveillance had not yet expired.

187. On 28 June 2022, DG ITEC of the European Parliament checked Androulakis 'phone and found the evidence of the attempted Predator hack of September 2021, and informed Mr Androulakis accordingly.[344] Androulakis filed a criminal report to the prosecutor's office of the Supreme Court on 26 July 2022.[345]

[333] InsideStory. From Koukakis to Androulakis: A new twist in the Predator spyware case.
[334] InsideStory. From Koukakis to Androulakis: A new twist in the Predator spyware case.
[335] Inside Story. From Koukakis to Androulakis: A new twist in the predator spyware case.
[336] BBC. Greece wiretap and spyware claims circle around PM Mitsotakis.
[337] News 24 7. Wiretapping scandal: Lawsuit against Intellexa by Thanasis Koukakis.
[338] Heinrich Boll Stiftung. In conditions of absolute loneliness
[339] InsideStory. From Koukakis to Androulakis: A new twist in the Predator spyware case.
[340] Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.
[341] Tovima. Androulakis lashes out at PM, ND spokesman says Pasok leader should say why his phone was tapped.
[342] Kathimerini. Surveillance hypothesis: the data that triggered the developments.
[343] WSWS. Greece's secret service illegally tapped phone of leader of social democratic PASOK party.
[344] Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.
[345] News 247. Nikos Androulakis: Near-Victim of Predator Software - Filed a Lawsuit.

Obtenu pour vous par
Got for you by
agence europe

188. A few days later, on 29 July, Androulakis presented the information about the Predator attack to the ADAE. At the same day, the Permanent Committee on Institutions and Transparency heard EYP chief Panagiotis Kontoleon and Christos Rammos, President of the ADAE, in the presence of the Ministers of Digital Governance and State. The meeting took place behind closed doors.[346]

189. On 8 September 2022, Androulakis asked the ADAE to hand over his wiretapping files.[347] However, on this same day, it becomes clear that the files of both Androulakis and Koukakis were destroyed by the EYP.[348] The destruction is an unequivocal fact, but the story behind the destruction remains unclear. On the one hand, some sources blame the destruction of the files on the change in the electronic systems of the EYP in 2021.[349] This change to the new legal assembly system allegedly caused a technical problem resulting in the destruction. On the other hand, other sources claim that Kontoleon gave the order on the 29 July 2022 to destroy these files on the same day that Androulakis informed the ADAE about the surveillance attempts.[350]

190. On the 5th of August, Kontoleon and Dimitriadis resigned from their positions. On the 8th of August Mitsotakis made a television statement, acknowledging the wiretapping of Androulakis, but reiterating the fact that he was unaware of the surveillance.[351]

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

192. Surveillance of a politician is highly unusual, and the Greek Constitution foresees special protection of politicians. The EYP denies any involvement in the surveillance with Predator. The Government initially floated suggestions about foreign powers that supposedly requested the wiretapping of Androulakis, or they suggested that his membership of an EP committee in charge of relations with China might be the reason. None of these hypotheses were very credible. The surveillance occurred in a political context of upcoming elections. Polls predicted that Néa Demokratía would lose its absolute majority. PASOK would be the preferred coalition partner. In autumn 2021, there were four candidates in the PASOK leadership contest, each with different views on such a coalition. Androulakis was said to be open to the idea, but not under the Premiership of Mitsotakis. Another candidate, Andreas Loverdos, had served earlier as a Minister in a Néa Demokratía - PASOK coalition, and was thought to be more supportive. He was acquainted to Dimitriadis. Manolis Othonas, the right hand of another candidate, was also said to be among those who had closer relations with Néa Demokratía and Dimitriadis. The publication of the list of other alleged targets by Documento, reinforces the suspicion of political reasons for the surveillance. There is no

[346] Avgi. Predator scandal / EYP dragged to Parliament over surveillance.
[347] Ekathimerini. Androulakis asks ADAE for his wiretapping file.
[348] TaNea. The archive of the surveillance of Nikos Androulakis destroyed.
[349] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.
[350] Ieidiseis. SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.
[351] Reuters. Greek PM says he was unaware of phone tapping of opposition party leader.

Obtenu pour vous par
Got for you by
agence europe

proof for any of these hypotheses, but it is essential that these avenues are investigated and eliminated where possible.

Stavros Malichoudis

193. 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.[352][353] 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.[354]

194. On 15 November 2021, government spokesperson Giannis Oikonomou indirectly confirmed the claims. He stated that the EYP could wiretap individuals if there is a risk to national security from "internal or external threats".[355] However, on 24 November and 17 December 2021, Minister of State George Gerapetritis denied any surveillance of journalists in Greece, including of Malouchidis, but he did not deny the authenticity of the EYP internal documents.[356]

195. During the PEGA hearing on Greeceon 8 September 2022,], Malichoudis stated that through wiretapping his phone, the EYP could also collect information from colleagues and journalists that he was in contact with during that time.[357] The EYP could have allegedly listened in on conversations Malichoudis had with the International Organisation for Migration (IOM)[358], pointing out the dangers for others, the so-called 'by-catch', of wiretapping an individual. In addition, during the hearing Malichoudis showed evidence that the EYP was interested in his work and sources, but that the reason for the monitoring is covered by "national security".[359]

Christos Spirtzis

196. 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.[360] Spirtzis had submitted critical parliamentary questions to the government on the surveillance tasks of the EYP on 15 November 2021. That same day he received a similar message as the one Nikos Androulakis had received. On 19 November, a second message was sent to Christos Spirtzis containing a link to an article of Efimerida ton Syntakton.[361] On 9 September 2022,

[352] Efsyn. Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ
[353] Solomon. Solomon's reporter Stavros Malichudis under surveillance for "national security reasons".
[354] BalkanInsight. Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.
[355] BalkanInsight. Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.
[356] https://wearesolomon.com/mag/accountability/solomons-reporter-stavros-malichudis-under-surveillance-for-national-security-reasons/
[357] European Parliament. Hearing September 8, 2022.
[358] BalkanInsight. Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.
[359] European Parliament. Hearing September 8, 2022.
[360] Ekathimerini. Former SYRIZA minister says he was targeted by Predator.
[361] Ekathimerini. Former SYRIZA minister says he was targeted by Predator.

Obtenu pour vous par
Got for you by
agence europe

Citizen Lab informed Christos Spirtzis of the attempted hacking, after which he lodged a complaint to the prosecutor of the Supreme Court.[362][363] Spirtzis is a confidante of party leader Tsipras, and present during high-level meetings of the party leadership.

Tasos Telloglou, Eliza Triantafyllou and Thodoris Chondrogiannos

197. Tasos Telloglou and Eliza Triantafylou have allegedly been spied upon during their investigative work for the Inside Story. In an article for the Heinrich-Böll-Stiftung on 24 October 2022, Telloglou shared his surveillance and intimidation experiences whilst investigating the surveillance scandals in Greece. According to these experiences, he believes to have been monitored between May and August 2022.[364]

198. In addition, a source from the security services had told Telloglou in June 2022 that the locations of him and his colleagues Eliza Triantafyllou (InsideStory) and Thodoris Chondrogiannos (Reporters United) were monitored by the authorities, to assess which sources they were meeting.[365] At time of writing, the Greek government has not yet responded to the allegations.

Other targets

199. On 29 October 2022 reported that other politicians had been targeted with the Predator spyware, including a government minister who was not on good terms with the Prime Minister. In addition, another member of Néa Demokratía reportedly received a link for the instalment of Predator.[366] Mr Oikonomou - government spokesperson - has stated that the article lacks concrete evidence.[367]

200. On 5 and 6 November 2022 Documento reported on a list containing 33 names of persons targeted with Predator spyware.[368] 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 because it suggests that the abuse of spyware is systematic, large-scale, and part of a political strategy.

[362] Reuters. One more Greek lawmaker files complaint over attempted phone hacking.
[363] Euractiv. Another Greek opposition lawmaker victim of Predator.
[364] Heinrich-Böll-Stiftung. In conditions of absolute loneliness.
[365] MapMF. Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations.
[366] Ta Nea. Four illegal manipulations by suspicious center.
[367] Politico. Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.
[368] Documento, edition 6 November 2022.

Obtenu pour vous par
Got for you by
agence europe

I.D. Cyprus

201. 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.

202. In 2019 Cyprus was rocked by a scandal following an interview of Tal Dilian with Forbes, showing off his "Black Van" full of state of the art surveillance technology. In the investigations that followed, it emerged that he had received government authorisation for an experiment at the national airport, collecting personal data of passengers via the airport WiFi.[369]

203. The investigation into Dilian's WiSpear van displayed further that Cyprus has become a fertile ground for the experimentation of surveillance equipment by the Cypriot based companies themselves. According to the main opposition party AKEL, over 9.5 million mobile devices were illegally tracked within Dilian's mass surveillance trial, violating many individual data protection rights.[370]

204. This incident may have political significance beyond the violation of the privacy of passengers. Given that Cyprus is situated on a cross-roads in many ways, there are several third countries that could potentially have an interest in having insight into the traveller movements through Larnaka airport: Turkey, Israel, Russia and the US, for example.

205. The court imposed a 76.000 euro fine on Dilian's company WiSpear, and the data protection authority issued a fine of 925,000 euro in light of GDPR violations.[371][372] However, the Attorney General dropped the cases against all individuals. The reasons for the decision not to prosecute them are classified, as is the report of the special inquiry that had been commissioned by the (previous) Attorney General. There is a remarkable contrast between the assertion on the one hand that the episode with the Black Van touches upon matters of national interest and critical infrastructure, and on the other hand the apparent light touch sanctions for the perpetrators.

206. There are close connections between Cyprus and Greece when it comes to the topic of spyware. Tal Dilian's Intellexa is established in Greece and his spyware Predator has been used in the Greek hacking scandals.

207. Besides the facilitation of a favourable export climate, the Cypriot government has allegedly used surveillance systems itself, although less is known about the victims compared to the other Member States, nor is it clear if spyware has been used or other surveillance methods,

[369] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[370] Kathimerini. 9.5 million mobile phones tapped in Cyprus according to AKEL.
[371] CyprusMail. Israeli company that deployed 'spy van' fined €925,000 for data violations.
[372] Financial Mirror. Spy van company fined €76,000.

Obtenu pour vous par
Got for you by
agence europe

or both. Journalist Makarios Drousiotis was reportedly monitored by the government since February 2018.[373] The government has denied the surveillance.

208. 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.

209. 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

210. The Ministry of Energy, Commerce and Industry in the Strategic Items Export Licensing Section regulates the export of dual use items.[374] In response to the PEGA questionnaire that was sent to all Member States, Cyprus stated that it monitors and assesses all export license applications for dual-use goods on a case-by-case basis, in full accordance with relevant sanctions regimes. These regimes are the European Union Global Human Rights Sanctions Regime, as well as the EU Regulation for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items [Regulation (EU) 2021/821], guided by the criteria of the relevant Council Common Position (2008/944/CFSP).[375] Cyprus is the only EU member state that is not signatory to the Wassenaar Arrangement, due to a Turkish veto. However, the government declares it is adhering to the same standards.

211. The Ministry of Energy, Commerce and Industry can consult the so-called Advisory Committee when it comes to permitting an export license. This committee consists of representatives from the Ministry of Defence, Ministry of Justice and Public Order, Ministry of Foreign Affairs, the Customs and Excise Department amongst other departments.[376] According to the Cypriot government, this committee is regularly consulted when export applications are examined. On several occasions, the export of dual-use goods to third countries has been rejected following a negative opinion of this committee.[377] The Chamber of Commerce usually does not provide information on the number of approved and rejected software-marketing licenses.[378]

212. During a meeting with the PEGA committee, Ministers Natasa Pilides and Kyriacos Kokkinos stated that there has been a sharp decline in the number of companies active in Cyprus. 32

[373] Makarios Drousiotis. Κράτος Μαφία. Chapter 5. Published 2022.
[374] http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument
[375] European Parliament questionnaire received from Cyprus.
[376] Lelaw. Export Controls for dual-use products.
[377] European Parliament questionnaire received from Cyprus.
[378] Inside Story. Who signs the exports of spyware from Greece and Cyprus?

Obtenu pour vous par
Got for you by
agence europe

companies are registered, but according to the Minister currently only 8-10 are active of which 3-4 produce spyware.[379]

213. In practice, Cyprus is reportedly rather lenient in providing spyware companies with export licenses.[380] 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.[381] 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.[382] Another way is to state that the product is exported for demonstration purposes only, although a detailed description of the product is added.[383]

214. Many Israeli companies come to Cyprus to start off their European activity.[384] Different sources reported furthermore that the country is home to approximately 29 Israeli companies.[385].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[386] as well as spyware materials from WiSpear.[387]

Ex-ante scrutiny

215. 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. An application for the issuance of an authorisation or extension of the interception of private communication by an authorised person is submitted to the Court by the Attorney General. The Chief of Police, the commander of the Cyprus Intelligence Service (KYP) or an investigative judge can request for such authorisation from the Attorney General.[388] Additionally, someone under or on behalf of the Attorney General of Cyprus cannot submit an application and no issuance of authorisation for the interception of private communication can be provided by a judge. Yet, these provisions can be overruled in cases where the interception of private communication is in the security interests of Cyprus, or to prevent, inquire or prosecute offences.[389]

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

[379] Meeting with Ms Natasa Pilides, Minister for Energy, Commerce and Industry and Kyriacos Kokkinos, Deputy Minister for Research, Innovation and Digital Policy during PEGA mission on 02.11.2022
[380] InsideStory. Who signs the exports of spyware from Greece and Cyprus?
[381] InsideStory. Who signs the exports of spyware from Greece and Cyprus?
[382] Philenews. This is how interception patents are exported from Cyprus.
[383] Philenews. Export of monitoring software confirmed.
[384] Philenews. Revelations in Greece: Predator came from Cyprus.
[385] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022
[386] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[387] Inside Story. Predator: The "spy" who came from Cyprus.
[388] CyLaw. The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996)
[389] CyLaw. The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996)

Obtenu pour vous par
Got for you by
agence europe

employees of their service, or employees carrying out assignments for their service, to intercept private communication and/or get access to the monitoring equipment for the sake of technical work.[390]

217. In addition, article 4(2) of Law 92(I)/1996 as amended in 2020[391], stipulates that if a device or machine has been primarily designed, produced, adapted or manufactured in order to allow or facilitate the interception or monitoring of private communication, no person is allowed to import, manufacture, advertise, sell or otherwise distribute such devices or machines. Violation of this article can lead up to a fine of 50 000 euro and/or up to 5 years imprisonment.[392] These provisions do not apply if the provider has informed the Central Intelligence Service (KYP), the Police and the Commissioner and secured their approval. These provisions do also not apply to the surveillance systems used by the Chief of the Police and the Commander of the KYP.[393]

Ex-post scrutiny

218. In Cyprus, the Processing of Personal Data (protection of individuals) law from 2001 outlines that if personal data is used or if an individual has been the subject of processing, the individual in question has the right to be informed.[394] This right can be circumvented once the Commissioner for the Protection of Personal Data decides otherwise in light of national security reasons amongst others.[395]

219. Moreover, the Protection of the Confidentiality of Private Communication Law as agreed on in 1996, spells out that in case of interception of private communications by law enforcement agencies, the Attorney General is obliged to inform the individual in question. Notifying the individual must occur within a maximum period of 90 days from the start of the issuance of the judicial warrant[396], or within a maximum period of 30 days as of the execution of this judicial warrant. The Attorney General must provide the individual in question with a report detailing the fact of the issuance of the court warrant, the date of the issuance of the court warrant and the fact that within this period, interception or access to private communications has occurred. This obligation can be delayed if the Attorney General decides that withholding this information is in the interest of the security of Cyprus, amongst others.[397] The Court can also order for non-disclosure of the information in light of security interests of Cyprus.[398]

[390] CyLaw. The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996)
[391] CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020
[392] European Parliament questionnaire received from Cyprus.
[393] European Parliament questionnaire received from Cyprus.
[394] CyLaw. The Processing of Personal Data (Protection of Individuals) Law of 2001 (138(I)/2001).
[395] Franet EU. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies. Legal update.
[396] CyLaw. Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).
[397] Franet EU. National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies. Legal update.
[398] CyLaw. The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996)

Obtenu pour vous par
Got for you by
agence europe

220. 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.[399] 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.[400]

Redress

221. The legality of the actions of the Cyprus Intelligence service are evaluated by a three-member committee as outlined in the Cyprus Intelligence Service Law 74(I)/2016. The tripartite committee is appointed by the Council of ministers, following a recommendation by the President of the Republic.[401]

222. The law of 92(I)/1996 was amended in 2020 and strengthened the oversight framework of the Republic, in particular the provisions concerning the tripartite committee. In the remit of its mandate, the committee can initiate ex officio inquiries and can start investigations into the facilities, technical equipment and archived material from the KYP. As introduced by the Article 17A(1) of Law 92(I)/1996 as amended by Law 13(I)/2020, the committee can also start inquiries into the Police 'facilities, technical equipment and archived material. In light of such investigations, the committee can appeal to the Attorney-General, the Commissioner for Personal Data Protection, or the Commissioner of Electronic Communications and Postal Regulation for further action. The Committee also provides the President of the Republic with an annual report, in which it outlines the activities, formulates observations and recommendations and identifies omissions.[402][403]

223. 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 send out to the President. At the time of writing, there is no information on the exact composition of the committee, its work and the scrutiny it performs.[404]

Key figures in the spyware industry

224. 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.[405] Tal Dilian served in different leadership

[399] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[400] Phileneως. Legal but uncontrolled interceptions.
[401] European Parliament questionnaire received from Cyprus.
[402] European Parliament questionnaire received from Cyprus.
[403] CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020
[404] Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.
[405] 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

Obtenu pour vous par
Got for you by
agence europe

positions in the Israeli Defence Force for 25 years before he retired from the military in 2002.[406] 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.[407]

225. In Cyprus, Dilian got closely associated with Abraham Sahak Avni. Avni has formerly been involved in the Israeli Police Special Forces as special detective.[408] In November 2015, he acquired Cypriot citizenship and a golden passport because of a 2.9 million euro investment in real estate.[409] Avni founded the Cypriot NCIS Intelligence Services ltd[410], a company that was reportedly involved with the most powerful technology-oriented companies in the world. [411] 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.[412] Government Party DISY (Dimokratikós Sinagermós) is also part of the company's clientele. Reportedly, Avni had installed security equipment in the party's offices.[413] Next to Avni's security equipment, Dilian's materials were also sold to the Cyprus Drug Enforcement Agency and the Cypriot Police.[414]

226. At one point, the Headquarters Crime Investigation Department of the Police found violations of the confidentiality of private communications related to Avni's company. The police however decided to close the case.[415]

227. The connections between Dilian and Avni are numerous. Dilian's company WiSpear shared a building in Lacarna and some of its personnel with Avni.[416] 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[417] and is also part of Intellexa Alliance. Reportedly, Sahak's relations with the DISY party created the testing ground for Dilian's products.[418]

Dilian's spyware van

228. 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'.[419] 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

[406] https://taldilian.com/about/
[407] Opencorporates. Passitora ltd.
[408] ShahakAvni. About Shahak Avni.
[409] Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.
[410] Philenews. FILE: The state insulted Avni and Dilian.
[411] Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.
[412] Philenews. FILE: The state insulted Avni and Dilian.
[413] Tovima. The unknown "bridge" between Greece and Cyprus for the eavesdropping system.
[414] Inside Story. Predator: The "spy" who came from Cyprus.
[415] Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.
[416] Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.
[417] CyprusMail. Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.
[418] Inside Story. Predator: The "spy" who came from Cyprus.
[419] https://intellexa.com/

Obtenu pour vous par
Got for you by
agence europe

assortment of surveillance software and services that Intellexa can offer and combine to its clients.[420] More detailed information on the corporate structurein the chapter on the Spyware Industry.

229. On 5 August 2019, Dilian gave an interview to Forbes magazine about his black WiSpear van, showing off the different spyware capabilities that his alliance offers. This 9 million euro worth van was capable of hacking devices within a range of 500 meters.[421] The public attention generated by the Forbes interview[422] led to an investigation by the Cypriot authorities. Lawyer Elias Stefanou was appointed as independent criminal investigator for this investigation. During this inquiry, the authorities discovered another one of Dilian's undertakings that included Larnaca International Airport.[423]

230. On June 16 2019, Tal Dilian reportedly entered into a non-contractual arrangement with Hermes Airports to use his WiSpear equipment for the alleged purpose of enhancing the Wi-Fi signal for passengers at Larnaca International Airport, whereafter three WiFi antennas were installed.[424] Although not registered in Cyprus, Israeli company Go Networks was also involved in the negotiations leading up to the arrangement.[425] The true reason for the agreement was however to test WiSpear's interception technology. The intercepted data of passengers was saved in the airport server room, close in proximity to the WiSpear office in Larnaca as shared with Avni.[426] During the period of time when the antennas were operable, intercepted data was retrieved from 9.507.429 mobile devices.[427]

231. 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.[428] 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".[429][430] Recall that, as mentioned above, Dilian's companies, as stated by the Chamber of Commerce, have not received any export licenses in the last two years. At time of writing, it remains unclear who authorised these export licenses.[431]

232. The electronic data extracted from the confiscated equipment for the investigation was submitted for a three-level forensic examination, by the police, an academic expert, and Europol.[432] The van has remained in police custody, but it is not clear what has happened to

[420] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[421] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[422] Forbes. A Multimillionaire Surveillance Dealer Steps Out Of The Shadows ... And His $9 Million Whatsapp Hacking Van.
[423] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[424] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[425] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022.
[426] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022.
[427] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[428] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[429] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022.
[430] Philenews. Export of tracking software from Cyprus.
[431] Inside Story. Who signs the exports of spyware from Greece and Cyprus?
[432] Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022

Obtenu pour vous par
Got for you by
agence europe

the surveillance equipment. It is thought that it has been returned to Dilian, but there seems to be no confirmation.

233. At 15 November 2021, the case was brought before the Criminal Courts with WS WiSpear Systems ltd, Tal Dilian and two other WiSpear employees as defendants. Ultimately, Attorney General George Savvides upheld the case against the company WiSpear, but the criminal proceedings against Dilian and the employees were dropped.[433] The reasons for that decision are classified. However, the Attorney General could decide at any given moment to reopen the case against the three individuals.

234. WiSpear pleaded guilty to 42 charges and was fined with 76000 euros in the Assize court on 22 February 2022.[434][435] WiSpear confessed to charges of illegal surveillance of private communications and data protection violations.[436] The Court published its final decision, stating that: "The Assize Court noted and qualified that the infringement attributed to the company never involved any intent, hacking [or] wiretapping, stating that there was never any attempt or purpose to personalize any data. The court emphasized that no damage was caused to any individual person".[437] In addition to a fine imposed by the Assize court, Commissioner for Personal Data Protection Irini Loizidou Nicolaidou fined WiSpear with 925,000 euro in light of GDPR violations.[438][439]

235. 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[440] and was registered with the assistance of the former law firm of Savvas Angelides.[441] 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.[442] In a press release on 10 August 2022, the Deputy Attorney General distanced himself from the contact between "a relative of mine intended to do business with Mr. Shahak Avni." He declared that he nor his family has any connection with Tal Dilian and that if there were evidence of surveillance or interception in the case of Dilians' van, then the criteria for determining the course of the case would have been different.[443]

236. Opposition party AKEL expressed outrage over the cases against Dilian and staff being dropped, and denounced the legal decision as a cover-up by the Attorney General.[444] After all, the Cypriot government had reportedly purchased equipment from Dilian's company and one of the accused employees had allegedly worked for NSO, providing the KYP with instructions on how to use the Pegasus spyware.[445] Dropping the charges ensured that the

[433] Financial Mirror. Anger after 'spy van' charges dropped.
[434] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[435] Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022
[436] Financial Mirror. Spy van company fined €76,000.
[437] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[438] CyprusMail. Israeli company that deployed 'spy van' fined €925,000 for data violations.
[439] Financial Mirror. Spy van company fined €76,000.
[440] Politis. "Interceptions" file: Classified Police Report (2016) shows he knew everything about Avni
[441] Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022.
[442] Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.
[443] Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022.
[444] Financial Mirror. Anger after 'spy van' charges dropped.Le
[445] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.

Obtenu pour vous par
Got for you by
agence europe

information on the links between Dilian's company and the Cypriot government would remain protected.[446] 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

237. Following the episode of the van and the lawsuit, Dilian moved Intellexa's operations to Greece, although he never left Cyprus and is still a resident. Indirect links between several natural and legal persons as registered in Cyprus and Greece expose the facilitation of Dilian's businesses to Athens.[447] What follows are some of the names that are part of the Cyprus-Greece connections, although the main role of Intellexa SA in Greece is further explained in the chapter on Greece.

238. According to recent testimonies in light of the judicial investigations in the van case, lawyer Aleksandros Sinka has had significant influence in the move to Greece. Sinka - who formerly played a key role in the centre-right DISY party - apparently had good relations with both Dilian and Avni.[448] It appears that Sinka was also an acquaintance of former General Secretary of the Greek government Grigoris 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.[449] 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.[450]

239. The judicial investigations led to the transfer of Avni's and Dilian's activities in Poltrex to Yaron Levgoren. Levgoren is a permanent resident of Canada. He became the shareholder, as well as director and secretary of Poltrex. What is important here is that Levgoren is also linked to Intellexa in Greece.[451] According to his Linkedin he currently represents the in Greek-based Intellexa company Apollo Technologies.

NSO Group and Cyprus

240. Next to Intellexa Alliance, Cyprus was allegedly also home to NSO Group. In 2010 Tal Dilian, together with Boaz Goldman and Eric Banoun, launched the company Circles Technologies, specialised in the sale of systems that exploit SS7 vulnerabilities.[452] Six years later, Circles Technologies was sold to Francisco Partners for just under 130 million dollars of which 21.5

[446] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[447] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[448] Tovima. The unknown "bridge" between Greece and Cyprus for the eavesdropping system.
[449] EDS. 2003/2004 Bureau.
[450] Tovima. The unknown "bridge" between Greece and Cyprus for the eavesdropping system.
[451] Philenews. How the spyware scandal in Greece is related to Cyprus.
[452] Amnesty International. Operating from the Shadows.

Obtenu pour vous par
Got for you by
agence europe

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.[453]

241. According to the response from the Cypriot government to the PEGA Committee, the Department of Registrar of Companies and Intellectual Property does not include a registered legal entity of NSO Group. NSO Group does not hold shares in any legal entity registered in Cyprus. Six companies have either been established or bought by Board members of the NSO Group. In addition, the Pegasus spyware does not appear to have been developed in, nor officially exported from Cyprus.[454]

242. Part of this statement seems to be true. Expansion under Francisco Partners between 2014 and 2019 did include six Cypriot companies. Francisco Partners was supplemented with ITOA Holdings Ltd., registered in Cyprus and parent company of CS-Circles Solutions Ltd., Global Hubcom Ltd. and MS Magnet Solutions. Ms Magnet Solutions owns Mi Compass Ltd. CS-Circles Solutions Ltd. furthermore owns CI-Compass Ltd. In addition to the Cypriot entities, CS-Circles Solutions Ltd. also owns Bulgarian entities. NSO Group has stated that "[...] The Bulgarian companies provide, on a contract basis, research and development services to their respective Cypriot affiliates and export the network products for governmental use."[455]

243. 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.[456] 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.[457]

244. 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 dollars.[458][459] It should be noted here that a year later, on 2 October 2018, the Saudi regime killed Jamal Khasoggi in the Saudi consulate in Turkey, after surveiling him and his near ones with Pegasus.

[453] Amnesty International. Operating from the Shadows.
[454] European Parliament questionnaire received from Cyprus.
[455] Amnesty International. Operating from the Shadows.
[456] Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.
[457] Akel report. PEGA mission to Cyprus.
[458] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[459] Haaretz. Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals.

Obtenu pour vous par
Got for you by
agence europe

245. According to CitizenLab, 25 state actors were clients of Circles Technologies in 2020. Amongst these state actors were Belgium, Denmark, Estonia and Serbia.[460] As of 2020, NSO Group has closed their Circles office stationed in Cyprus. At the time of writing, it remains unclear which Circles 'companies remain operable.[461]

Black Cube

246. 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. In 2018, the three lawyers received several messages from so-called acquaintances of certain firms and individuals, proposing meetings in London. Hulio stated, "For the lawsuit in Cyprus, there was one involvement of Black Cube" since the lawsuit "came from nowhere and I want to understand".[462] Black Cube was also exposed in spying scandals in Hungary and Romania.

Purchase and use of Spyware by Cyprus

247. 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.

248. After the elections of 2013, Andreas Pentaras was appointed as head of the Cyprus Intelligence Service whilst surveillance expert Andreas Mikellis was responsible for the protection of President Anastasiades' communications. In that same year, Mikellis reportedly visited the ISS surveillance exhibition in Prague, where he allegedly negotiated with Hacking Team for the purchase of the so-called DaVinci software.[463] The DaVinci software was able to infect applications of a mobile phone and therefore did not meet the official requirements for the lifting of privacy.[464]

249. Disclosed contact information as revealed by WikiLeaks between Mikellis and Hacking Team indicated the bypassing of tender procedures and lack of proper review of the acquired surveillance system. At the start of 2014, the software was reportedly installed and four employees of the KYP were trained, including Mikellis.[465]

250. When WikiLeaks revealed the purchase of Hacking Teams' surveillance software, the KYP confirmed that this system was only used for national purposes only.[466] Despite Mikellis

[460] CitizenLab. Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles.
[461] Amnesty International. Operating from the Shadows.
[462] The New Yorker. How Democracies Spy on their Citizens.
[463] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[464] Inside Story. Predator: The "spy" who came from Cyprus.
[465] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[466] Inside Story. Predator: The "spy" who came from Cyprus.

Obtenu pour vous par
Got for you by
agence europe

contact with Hacking Team[467], it was the head of the KYP Andreas Pentaras who ultimately resigned after these revelations came to light.[468] Kyriakos Kouros replaced Pentaras.

251. Another detail of WikiLeaks that is of interest here is that one more other police department was also interested in purchasing a communications surveillance system from Hacking Team. This department tried to secure this system through Sahak Avni.[469]

Victim Makarios Drousiotis

252. 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.[470]

253. In the course of Drousiotis 'inquiries into the Russian connections, revelations about NSO Group operating from Cyprus started to appear in international media outlets, including on the Pegasus 3 presentation in the Four Season Hotels. CitizenLab moreover suspected Cyprus to be one of the countries using the NSO technologies for the sake of communication interception of the British Foreign Office computer systems.[471] At this point, Drousiotis started to recall several indications of the Pegasus spyware infiltrating his telephone, including a missed WhatsApp call, rapid battery depletion and the frequent overheating of his device without him using it.[472] In light of these events, Drousiotis believes the Cypriot government - more particularly the Cyprus Intelligence Service - to be behind the infection of his phone.

254. In May 2019, Drousiotis sent a letter to President Anastasiades expressing his concerns around the surveillance of his phone, outlining the potential motives behind this surveillance as well as holding the President personally accountable for whatever may happen to him after the espionage. Anastasiades forwarded the letter to the current head of the Cyprus Intelligence Service Kyriakos Kouros. Both Anastasiades and Kouros have refuted the alleged surveillance with the Pegasus software, reiterating that NSO Group was in fact not even registered in Cyprus.[473]

255. In the months that followed, several intimidation attempts occurred including the disappearance of evidence on his computer, the disconnection of security camera's at Drousiotis home and being tracked by strangers. After going public with his story and submitting a complaint at the Cypriot police office, Drousiotis got in touch with Lambros Katsonis Head of the Technical Support Department of Panda Security, a Cypriot company specialised in antivirus equipment. Drousiotis was however unware of the fact that the Cypriot

[467] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[468]CyprusMail. Intelligence chief resigns after spy tech revelations. https://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/
[469] Inside Story. Predator: The "spy" who came from Cyprus.
[470] Makarios Drousiotis. Κράτος Μαφία. Chapter 5. Published 2022.
[471] BBC. No 10 network targeted with spyware, says group.
[472] Makarios Drousiotis. Κράτος Μαφία.. Chapter 5. Published 2022.
[473] Makarios Drousiotis. Κράτος Μαφία.. Chapter 5. Published 2022.

Obtenu pour vous par
Got for you by
agence europe

government also used this antivirus software for their own devices. Against this background, Katsonis seems to have been sent to Drousiotis home under false pretences. Possibly with the aim to further infiltrate Drousiotis devices as instructed by the Cypriot Intelligence Service (KYP).[474]

256. As of spring 2019, Drousiotis became aware of the suspicious entries in his Android phone and reached out to Google One Support to confirm the nature of these entries. Yet, Google does in general not respond to surveillance related matters, referring the customer in question to the national law enforcement agencies.[475] Mr Drousiotis, though not having any confidence in the police, did agree to hand over his devices for forensic examination.

Additional remarks

257. 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.

[474] Makarios Drousiotis. Κράτος Μαφία.. Chapter 5. Published 2022.
[475] Makarios Drousiotis. Κράτος Μαφία.. Chapter 5. Published 2022.

Obtenu pour vous par
Got for you by
agence europe

I.E. Spain

258. 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.[476] The targeting of a second group of victims is referred to as "CatalanGate".[477] It includes Catalan parliamentarians, Members of the European Parliament, lawyers, civil society organisation members and some family and staff connected to those victims.[478] 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.[479] In May 2020, the Spanish authorities admitted to targeting 18 of those 65 victims with court authorisation.[480]

259. The Spanish government has given little information so far on their role in this targeting, invoking the need for confidentiality in relation to national security. However, on the basis of a series of indicators it is generally assumed that the surveillance of the Catalan targets was conducted by the Spanish authorities, mainly in connection with the 1 October 2017 independence referendum in Catalonia, and ensuing events.[481] [482] The Spanish government was probably the first EU customer of NSO group.[483] [484]

260. A close analysis of the attacks shows a clear pattern. Most of the "CatalanGate" attacks coincide with, and relate to moments of political relevance, such as court cases against Catalan separatists, public rallies, and communication with Catalan separatists living outside Spain.[485] Such surveillance includes for example the lawyer-client communications of a jailed separatist on the eve of his trial, contacts between partners, or communications relating to the taking up of seats in the European Parliament. Given that the authorities have acknowledged only 18 out of 65 cases, and that the warrants for those cases are not disclosed, it is not possible

[476] Le Monde, https://www.lemonde.fr/en/international/article/2022/05/10/spain-fires-head-of-intelligence-services-over-pegasus-phone-hacking_5982990_4.html , *10 May 2022.*
[477] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022*.
[478] 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.
[479] 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.
[480] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , *5 May 2022.*
[481] 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.
[482] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022* at pg. 3.
[483] Vice, https://www.vice.com/en/article/pkyzxz/spain-nso-group-pegasus-catalonia , *14 July 2020.*
[484] Vice, https://www.vice.com/en/article/pkyzxz/spain-nso-group-pegasus-catalonia , *14 July 2020.*
[485] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022.*

Obtenu pour vous par
Got for you by
agence europe

to establish in what way they would have an immediate impact on, or constitute an imminent threat to national security or the integrity of the state.[486]

Purchase of Spyware

261. 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 Centre (CNI) and police has been widely publicised.[487] It was also previously reported by CitizenLab that Spain was a suspected customer of Finfisher.[488] In 2020, the Spanish newspaper *El Pais* reported that Spain has done business with NSO Group and that the CNI routinely uses Pegasus.[489] The Spanish government allegedly purchased the spyware in the first half of the 2010s for an estimated amount of €6 million.[490] [491] 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.[492]

262. Reportedly, the Spanish government was also exploring the idea of purchasing Predator spyware from Intellexa Alliance. Documents dating 1 July 2022 have been leaked, containing details on what services Intellexa offer for what price, accompanied by a brochure for their spyware in Spanish.[493] In the documents, it is clearly visible just how intrusive this spyware can be, with specific details on which phone models are susceptible and how far back the retroactive spying can stretch.[494] However, there has been no confirmation to date as to whether or not the Spanish government or secret services have acquired the tool.

Legal Framework

263. 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'.[495] 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.[496] The constitution also provides further exceptions to those rights in Part I Section 55 by stating that some freedoms

[486] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022*.
[487] 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.
[488] 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.
[489] 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.
[490] Politico, https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/ ,*20 April 2022.*
[491] 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.*
[492] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , *18 April 2022.*
[493] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/
[494] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/
[495] Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx , at Section 18.
[496] Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx , at Section 18.

Obtenu pour vous par
Got for you by
agence europe

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.[497]

264. Further detail on the exemptions to the Article 18 right to privacy is outlined in the Criminal Procedure Act.[498] Article 588 of the Act requires authorisation to be provided by a judge, subject to four specific principles. Firstly, speciality (that the surveillance is related to a specific crime). Secondly, adequacy (outlining duration, objective and the subjective scope). Thirdly, proportionality (strength of existing evidence, severity of the case and result sought), and finally the exceptional nature and necessity (there are no other measures available and without it, the investigation will be interfered with).[499]

265. Article 197 of the Criminal Code sets out a four-year prison sentence for persons who seize or intercept *i.a.* electronic mail and telecommunications without correct permission.[500] Additionally, Article 264 of the Code of Criminal Procedure further regulates this area in relation to the criminal act of erasing or deleting of data, but does not criminalise the act of gaining access to the data itself in situations where the required authorisation has been granted.[501]

266. 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.[502] 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. [503] [504]

267. Despite the fact that the Spanish legislative framework appears to have given significant consideration to the necessity of judicial consent for surveillance, there still appears to be a major gap in the law relating to the retroactive nature of spyware. Even with the legal requirement for the duration of the surveillance to be specifically stipulated before authorisation, this does not provide for the fact that once a device is infected with spyware, it

[497] Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx , at Section 55.
[498] Criminal Procedure Act 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf .
[499] Criminal Procedure Act, 2016 https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf at Article 588.
[500] Criminal Code 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf , at Article 197.
[501] Criminal Procedure Act, 2016 https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf at Article 264.
[502] https://www.cni.es/en/intelligence
[503] https://emad.defensa.gob.es/en/?_locale=en
[504] Geneva Centre for Security Sector Governance report 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf at pg. 40.

Obtenu pour vous par
Got for you by
agence europe

is possible to retroactively review past communications and data in a way that was not possible with traditional surveillance measures.

Ex-ante Scrutiny

268. 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.[505] The CNI was established under Law 11/2002 May 6 and it authorises the CNI to conduct 'security investigations'.[506] However, there is little clarification on the means or limitations of such activities.[507] Law 11/2002 also established parliamentary, executive and legislative oversight control over the CNI [508] Parliamentary oversight is to be carried out by the Official Secrets Committee of the Spanish Congress, which was established in 1995.[509] The Delegated Committee for Intelligence Affairs is in executive control of the body, and co-ordinates the intelligence activities of the CNI.[510] Lastly, the Defence Committee of the Congress of Deputies conducts legislative oversight over the CNI.[511] The annual Intelligence Directive dictates the intelligence priorities of the CNI for the year.[512]

269. Judicial control over the actions of the CNI is provided for in Organic Law 2/2002 May 6.[513] [514] It states that a Magistrate of the Supreme Court may grant authorisation for measures taken in violation of the right to privacy of communications.[515] These provisions were brought in to force at a time when surveillance technology was far less advanced, and spyware such as Pegasus and Candiru did not exist. The legal safeguards risk therefore being outdated and do not provide citizens with sufficient protection.

270. The Official Secrets Act of 1968 originates in the Franco regime era and its reform has been long debated in Spain. The biggest issue with this largely antiquated piece of legislation is that it does not outline a time period beyond which the imposed secrecy would expire.[516] [517]

---

[505] 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.
[506] 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.
[507] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain , *4 May 2022.*
[508] 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.
[509] Law 11/1995 May 11, https://www.boe.es/eli/es/l/1995/05/11/11/con .
[510] 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.
[511] 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.
[512]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.
[513] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain , *4 May 2022.*
[514] Organic Law 2/2002 May 6, https://www.global-regulation.com/translation/spain/1451142/law-2-2002%252c-6-may%252c-regulating-the-prior-judicial-control-of-the-national-intelligence-center.html .
[515] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain , *4 May 2022.*
[516] El Pais, https://english.elpais.com/spanish_news/2021-04-05/spanish-government-begins-reform-of-franco-era-official-secrets-law.html , *5 April 2021.*
[517] Official Secrets Act of 1968,

Obtenu pour vous par
Got for you by
agence europe

Ex-post Scrutiny

271. 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.[518]

272. As result of the revelation that the CNI has used Pegasus and Candiru, the Spanish Ombudsman began conducting an investigation. However, this investigation was only concerning the 18 persons that the Spanish authorities have confirmed they targeted with court authorisation.[519] [520] Moreover, the Ombudsman does not deal with issues regarding the CNI, but rather only the police. The result of the investigation was to conclude that everything was done within the law[521] and to recommend a review of the existing legal provisions and make reforms where necessary to reflect the modernisation of surveillance systems.[522] On foot of this, the Spanish government announced in May 2022 that there would be a review conducted on the Official Secrets Act of 1968, and the Organic Law Regulating Prior Judicial Control of the CNI (Law 2/2002).[523]

273. 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 for targeting.[524] The hearing was not public and those present were not allowed to enter with any electronic on them whatsoever.[525] According to the spokespersons present at the hearing, it was almost solely focused on the Catalan victims and not on Pedro Sanchez or Margarita Robles and the alleged 3GB of data that was taken from their devices by mercenary spyware.[526] Robles has repeatedly insisted that the targeting of the 18 Catalans was valid owing to the 'situations of violence against people' following the Supreme Court sentencing nine key pro-independence figures to jail.[527]

---

[518] 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.
[519] The Guardian, https://www.theguardian.com/world/2022/may/05/catalans-demand-answers-after-spanish-spy-chief-confirms-phone-hacking , *5 May 2022.*
[520] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , *5 May 2022.*
[521] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx , *26 May 2022.*
[522] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx , *26 May 2022.*
[523] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx , *26 May 2022.*
[524] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , *5 May 2022.*
[525] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , *5 May 2022.*
[526] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , *5 May 2022.*
[527] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , *5 May 2022.*

Obtenu pour vous par
Got for you by
agence europe

274. Sanchez has also spoken on the issue in the Spanish Lower House where he once again reiterated that everything has been done within the law, and that the national security is subject to the control of the Parliament and other government bodies.[528] The idea that the use of Pegasus by the CNI was all legal was also claimed by former NSO Group CEO, Shalev Hulio, who told the New Yorker that the use of Pegasus by Spain was legitimate given Spain's strong respect for the rule of law and requirement for Supreme Court authorisation.[529]

Public Scrutiny

275. 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.[530]

Redress

276. A legal case regarding the surveillance of Prime Minister Sanchez and Minister for Defence Robles was filed in Madrid in the Audienca Nacional, the Spanish National Court (SNC), by the state solicitors' office.[531] Judge Jose Luis Calama, head of the Central Court of Instruction number 4, is responsible for this on-going case.[532] 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.[533]

277. 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 Catalonian victims of spyware are moving at a slow pace.[534] [535] The first case in Investigative Court number 32 in Barcelona was filed by two Pegasus victims in 2020; former President of the Catalonian 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

[528] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx , *26 May 2022.*
[529] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , *18 April 2022.*
[530] Dit Kan Geen Toeval Zijn, De Volkskrant podcast series by Huib Modderkolk and Simone Eleveld, 2022.
[531] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022.*
[532] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022.*
[533] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022.*
[534] El Diario, https://www.eldiario.es/catalunya/juez-barcelona-no-ve-base-imputar-empresa-pegasus-espionaje_1_9068271.html , *9 June 2022.*
[535] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html , *30 May 2022.*

Obtenu pour vous par
Got for you by
agence europe

Council, Ernest Maragall.[536] 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 virtually 'paralysing 'the case.[537] 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.[538]

278. 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.[539] 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.[540]

279. There are a number of other pending legal cases linked to the 65 Catalonian 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.[541] [542] 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.[543]

Targets

280. The targeting of Catalan citizens with spyware reportedly began as early as 2015, and has been carried out on a large scale since 2017.[544] 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.[545]

---

[536] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022*.
[537] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html , *30 May 2022*.
[538] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022*.
[539] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022*.
[540] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022*.
[541] El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html , *3 May 2022*.
[542] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab , *19 April 2022*.
[543] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab , *19 April 2022*.
[544] https://catalonia.citizenlab.ca/#targeting-puigdemont
[545] 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.

Obtenu pour vous par
Got for you by
agence europe

281. Spanish Prime Minister Pedro Sanchez, Minister for Defence Margarita Robles and Minister of the Interior Fernando Grande-Marlaska were targeted with Pegasus between May and June 2021.[546] There is little information available so far on details of this hacking, as they were announced by the government and were not the result of an investigation of CitizenLab or any other such research service or investigative journalists. Sanchez 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 Sanchez and Robles were government-issued and were being scanned for spyware occasionally.[547] Grande-Marlaska was infected on his personal device.[548] 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.[549]

282. 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.[550] At least 51 individuals were successfully infected.[551] The director of the CNI, Paz Esteban, has previously acknowledged to the Official Secrets Committee that 18 of those 65 persons were hacked by the Spanish authorities with the required judicial authorisation from the Supreme Court.[552] The Spanish government have refused to comment on the remaining victims as to whether or not they were responsible for their targeting.[553] Included among the 18 alleged legal targets is the current President of Catalonia, Pere Aragones, former President and current MEP Carles Puigdemont and other pro-independence politicians and their associates.[554] The majority of those 18 persons were never charged with a crime, such as civil society organisation members, journalists and lawyers, 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.[555] All 65 Catalan targets have at some point in time been in contact with the Catalan separatists living outside Spain.

[546] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html , *2 May 2022*.
[547] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099 , *7 May 2022*.
[548] La Razon,
[549] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099 , *7 May 2022*.
[550] 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.
[551] 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.
[552] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html *5 May 2022.*
[553] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html *5 May 2022.*
[554] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html , *5 May 2022.*
[555] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html *5 May 2022.*

Obtenu pour vous par
Got for you by
agence europe

Members of the European Parliament

283. 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.[556] Two MEPs were directly infected, while three others were hacked through family and staff.

284. Diana Riba i Giner MEP of Esquerra Republicana de Catalunya (ERC) was directly infected with Pegasus spyware on 28 October 2019, only three months after taking her seat in the Parliament. Following a discussion with her assistant over the phone, Riba i Giner answered an anonymous phone call and heard a recording of the conversation she just had with her staff member. The timing of this infection directly coincided with a crucial court ruling on the Catalan separatists, one of whom is Raül Romeva, husband of Riba i Giner who ultimately received a 12 year sentence.[557] Riba i Giner outlined at a hearing of the Pegasus Committee of Inquiry in the European Parliament that at that time, the majority of her phone calls were regarding the court case, as well as carrying out countless meetings and visits to the Courts. As such, the by-catch in this instance was incredibly significant, including Romeva and those connected to the landmark case.[558]

285. Jordi Solé MEP, also of ERC was originally reported to have been hacked on both the 11th and 27th of June 2020 according to the research of CitizenLab.[559] However, five further attacks during the same period were later discovered.[560] Sole only discovered that he had been targeted with Pegasus by accident when, after receiving some potentially suspicious messages, he submitted his phone to be checked as part of a documentary.[561] [562]Similar to the case of his colleague, the timing of this targeting is worthy of note. It came during critical political discussions on the vacant seat of Oriol Junqueras, who was not granted permission to take up his position as an MEP while imprisoned in Spain for sedition,[563] and only one month before Solé was appointed to take over that seat in July 2020. Additionally, there were on-going discussions at that time on party strategy and international litigation regarding their imprisoned and exiled colleagues during the time of the infections.[564]

286. Antoni Comin i Oliveres MEP, of Together for Catalonia (JUNTS) and Vice President of the Council of the Catalan Republic, was directly infected with Pegasus spyware at least once in the period between August 2019 and January 2020. Again, the timing is significant given that

[556] 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.
[557] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Ms. Diana Riba i Giner MEP, Strasbourg 6 October 2022.
[558] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Ms. Diana Riba i Giner MEP, Strasbourg 6 October 2022.
[559] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022* at pg. 7.
[560] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Mr. Jordi Sole MEP, Strasbourg 6 October 2022.
[561] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , *18 April 2022*.
[562] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Mr. Jordi Sole MEP, Strasbourg 6 October 2022.
[563] Politico, https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/ , *9 January 2020*.
[564] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Mr. Jordi Sole MEP, Strasbourg 6 October 2022.

Obtenu pour vous par
Got for you by
agence europe

during that period, Comin i Oliveres was taking up his role as an MEP and organising a major event on the border of Catalonia and France in order to rally support for an independent Catalonia.[565] Comin i Oliveres was in constant contact with the Ministry of the Interior in France at the time, making the French government a significant by-catch.

287. Carles Puigdemont MEP for JUNTS and former President of Catalonia was a victim of relational targeting through his spouse Marcela Topor, members of staff and a number of his associates.[566] In total, CitizenLab report that up to 11 individuals in close contact with Puigdemont were targeted, including at least two confirmed infections on Topor's device on 7 October 2019 and 4 July 2020.[567]

288. Clara Ponsati MEP for JUNTS and former Minister of Education of Catalonia was also a victim of relational targeting. Pol Cruz, a staff member at the Parliament, was confirmed to have been infected on 7 July 2020.[568]

Catalonian Politicians

289. Former President of the Catalonian Parliament and current Minister of Business and Work Roger Torrent was among the first persons to come forward as a victim of the 2019 WhatsApp Pegasus infections.[569] 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.[570] All of the Presidents of Catalonia since 2010 have been targeted with spyware either during or after their term in office.[571] 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

290. Jordi Domingo was one of the first Catalonian 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

[565] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Mr. Antoni Comin i Oliveres MEP, Strasbourg 6 October 2022.
[566] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 April 2022* at pg.7.
[567] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ *18 April 2022* at pg.8.
[568] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ *18 April 2022* at pg.7.
[569] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware , *13 July 2020.*
[570] 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.
[571] Artur Mas (after leaving office), Carles Puigdemont (relational targeting), Joaquim Torra (while in office), Pere Aragones (infected while serving as Torra's Vice President). https://catalonia.citizenlab.ca/

Obtenu pour vous par
Got for you by
agence europe

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.[572]

291. CitizenLab discovered an active Candiru infection on the laptop of Joan Matamala, an activist with close ties to pro-independent Catalan politicians in February 2021.[573] Candiru is significantly harder to trace than Pegasus, and this discovery of an active infection allowed the researchers at CitizenLab to better understand its patterns. Subsequently, 16 other infections on Matamala's device were discovered.[574] Microsoft subsequently patched the vulnerabilities through updates but it is impossible to know the number of Candiru infections that have gone unnoticed.[575]

292. The Catalan NGO Omnium Cultural has been victim to some of the most extensive targeting of a civil society organisations in Spain to date.[576] Omnium played a role in the 2017 independence referendum. The targeting centred around the President of Omnium, Jordi Cuixart who was one of the nine persons to sentenced to prison by the Supreme Court for sedition following a rally he led in favour of the referendum.[577]

293. Catalan journalist and wife of Cuixart, Meritxell Bonet, was infected on 4 June 2019. At this time, Cuixart was coming to the end of his trial which would end on 12 June 2019 and Bonet was in constant contact with him as well as his legal team.[578] Bonet was also a routine visitor during Cuixart's time in prison as well as making daily phone calls to him.

294. Vice President of Omnium and journalist Marcel Mauri was potentially the most aggressively targeted from the organisation. Having taken over the as the public representative of Omnium while Cuixart was imprisoned, he was targeted 19 times with Pegasus between 2018 and 2020 with three of those being successful infections.[579] Mauri paid weekly visits to Cuixart in prison, and was attending many important strategy meetings with various stakeholders on behalf of Omnium.

Lawyers

295. Gonzalo Boye has represented many high profile Catalan figures, including former Presidents Puigdemont and Torras.[580] Over five months between January and May of 2020, he was a victim of Pegasus himself.[581] Boye was targeted as many as 18 times during that period via

[572] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware , *13 July 2020.*
[573] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , *18 April 2022.*
[574] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , *18 April 2022.*
[575] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , *18 April 2022.*
[576] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ , *18 April 2022* at pg.9.
[577] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ , *18 April 2022* at pg.9.
[578] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ , *18 April 2022* at pg.9.
[579] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ , *18 April 2022* at pg.9.
[580] https://catalonia.citizenlab.ca/
[581] https://catalonia.citizenlab.ca/

Obtenu pour vous par
Got for you by
agence europe

text messages that appeared as tweets from civil society organisations or prominent news outlets.[582] 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.[583] The targeting of Boye has called in to question the legality of attacking the lawyer-client privilege.

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

297. Andreu van den Eynde i Adroer, was successfully infected with Pegasus on 14 May 2020.[584] The hacking occurred while he was acting as the lawyer of both Raul Romeva and Oriol Junqueras in their case before the Supreme Court.

298. 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.

[582] https://catalonia.citizenlab.ca/
[583] https://catalonia.citizenlab.ca/
[584] 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.

Obtenu pour vous par
Got for you by
agence europe

I.F. Other Member States

299. 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.

300. 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.

301. 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.

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

303. 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.[585] 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.[586]

304. 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.

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

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

Obtenu pour vous par
Got for you by
agence europe

The Netherlands

306. 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.[587] 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.[588] No insight is given into the expenditure by both police and intelligence services for the purchase and use of the spyware system.

307. It should be noted that from November 2014 to December 2016, NSO Group was able to operate thanks to two companies, Shapes 1 BV and Shapes 2 BV, established in the Netherlands, in the sectors of "financial holdings" and "engineers and other technical design and advice." Both were liquidated again after two years in operation.[589]

308. 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. WiSpear had won a tender of the Dutch Ministry. It does not become clear from the mail exchange if it concerns Predator or another product. From disclosed emails exchanged between the Cypriot Ministry of Energy, Commerce and Industry and WiSpear, it becomes clear that a representative of the Dutch Ministry of Defence had contacted the Cypriot Ministry of Commerce to obtain assurances about WiSpear on 13-15 November 2019, only days before the "spy van" story of Dilian broke. Dilian informed the representative of the Cypriot Commerce Ministry that he appreciates her immediate assistance in the matter as the expiry of the timetable for contract signatures is approaching".[590] It is not clear whether or not the contract was signed and any spyware was provided to the Dutch Defence Ministry.

309. On 2 June 2022, the media reported that the AIVD (General Intelligence and Security Service) used Pegasus when it assisted the police in tracking down a suspect of serious crime, Ridouan T.[591] The Dutch government refused to comment. This is a remarkable case that merits closer attention. The leaks took place at a time when Pegasus and NSO Group were under a lot of public criticism, and the blacklisting by the US Department of Commerce hurt them financially. The Dutch success story of catching one of the nastiest criminals in years, was a welcome positive message. The media report is based on statements by four sources within the AIVD. Their motive for leaking is not mentioned in the report. Nor does there seem to be

[587] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/23/ntwoorden-op-kamervragen-over-het-gebruik-van-hacksoftware-zoals-pegasus-in-nederland
[588] https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021
[589] Amnesty International, Operating from the shadows: inside NSO Group's corporate structure, https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[590] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
[591] https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/

Obtenu pour vous par
Got for you by
agence europe

an investigation into these leaks, which raises the question if the leak had the approval of the AIVD management. It is however highly unlikely that the AIVD would allow for such a story to get out, without the knowledge and approval of the Israeli authorities.

Belgium

310. In an interview with The New Yorker, a former Israeli intelligence official revealed that the Belgian police uses Pegasus in its operations.[592] 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.[593]

311. El Mahjoub Maliha, a Belgian activist with origins from the Western Sahara, and Carine Kanimba, daughter of Rwandan political activist Paul Rusesabagina, have also been spied upon via Pegasus software while in Belgium, and even during meetings with Belgian government officials. The spyware attacks were most likely carried out by, or on behalf of, the Rwandan authorities. Other Belgian targets of the use of spyware include former PM Charles Michel and his father Louis Michel (then MEP, former Commissioner and Foreign Minister). According to Belgian media, the Moroccan government was behind the attacks.[594][595]

Germany

312. In September 2021, it was reported that the German Federal Criminal Police Office (BKA) had acquired Pegasus in late 2020. It is important to note here that German law distinguishes two forms of spyware use[596]: access all information (Online-Durchsuchung[597]) and access only live communication (Quellen-TKÜ[598]). 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.[599] Only after new negotiations, NSO agreed, so the BKA acquired a modified version.[600] 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.[601]

[592] https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens
[593] https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spionagetool-pegasus/10329450.html
[594] https://www.knack.be/nieuws/wereld/belgisch-slachtoffer-van-pegasus-spyware-mijn-leven-is-in-gevaar/
[595] https://www.knack.be/nieuws/pegasus-project-macron-en-michel-in-het-vizier-van-marokko/
[596]https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html
[597]https://www.gesetze-im-internet.de/stpo/__100b.html
[598]https://www.gesetze-im-internet.de/stpo/__100a.html
[599]https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html
[600]https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-103.html
[601] https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-prufbericht-zur-pegasus-software/

Obtenu pour vous par
Got for you by
agence europe

313. In October 2021, it was also revealed that the German foreign intelligence service, the Federal Intelligence Service (BND), also bought a modified version of Pegasus, although the acquisition was classified.[602]

314. In response to a parliamentary question, the Federal Government indicated that the use of Pegasus is only permitted in individual cases and in respect of strict legal conditions laid down in the German Code of Criminal Procedure (StPO), the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (G-10 Act), and the Federal Criminal Police Office Act (BKAG), but it did not want to comment further.[603]

Use of Finfisher

315. 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.

316. The BKA kept testing new versions of the spyware provided by FinFisher for it to be used only in a "legally secure and technically clean" manner, and only after five years, in 2018, the Federal Ministry of the Interior approved it to be used. This was during the same year as the use of FinFisher against opposition parties in Turkey was discovered. However, the contract between FinFisher and the Berlin police had already ended by then, so the police in the capital never used it. The BKA did not further comment on any use of FinFisher in its operations or if the contract is still valid.[604]

317. On 6 April 2022, it was reported that the German government's cyber acquisitions agency ZITIS was prospecting for available technologies elsewhere in the wake of the disgraced spyware company Finfisher's filing for bankruptcy.[605] Among others, it was reported that, since 2019, it had met 5 times[606] with the Italian surveillance company RCS Lab, but there was no proof of acquisition of a tool from RCS lab.[607]

Malta

318. 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:

[602] https://www.sueddeutsche.de/politik/pegasusprojekt-nso-pegasus-bundesnachrichtendienst-1.5433974
[603] https://dserver.bundestag.de/btd/19/322/1932246.pdf
[604] https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/
[605] https://www.intelligenceonline.com/surveillance--interception/2022/04/06/after-finfisher-s-demise-berlin-explores-cyber-tool-options,109766000-art
[606] answer to a parliamentary question by the Left Party MEP Martina Renner https://dserver.bundestag.de/btd/20/038/2003840.pdf
[607] https://netzpolitik.org/2022/rcs-lab-hackerbehoerde-trifft-sich-mehrmals-mit-staatstrojaner-hersteller/

Obtenu pour vous par
Got for you by
agence europe

319. Tal Dilian: Israeli citizen, formerly Israeli army, founder of Intellexa, living in Cyprus, has acquired a Maltese passport in 2017.[608] He also co-owns a company on Malta called MNT Investments LTD.[609][610]

320. Anatoly Hurgin: Russian-Israeli citizen, former Israeli military engineer, acquired Maltese passport in 2015.[611] He is the founder of Ability Ltd, which cooperated with NSO Group on Pegasus and handled the network side of operations of NSO.[612][613] At the time of his application for a Maltese passport, he was already under investigation for various crimes.[614] Investigative journalist Daphne Caruana Galizia, who was later murdered in October 2017, wrote about him in August 2016.[615] In 2017, Ability Ltd was under investigation by the US Securities and Exchange Commission for allegedly lying about the state of its finances, and it was also almost delisted by NASDAQ.[616] Hurgin reportedly also owns a company in Lithuania, called UAB "Communication technologies", in the area of "connection and telecommunication services".[617]

321. Felix Bitzios: Director of Malta based company Baywest Business Europe Ltd[618]; formerly owner and employee of Intellexa; involved in the Piraeus/Libra fraud case[619];

322. Stanislaw Szymon Pelczar: legal representative of Baywest Business Europe Ltd; formerly administrator of Krikel; mentioned in the Paradise Papers[620];

323. Peter Thiel: German-born, American citizen, acquired New Zealand citizenship in 2011 despite not residing in there; has applied for a Maltese Golden Passport in 2022 (shortly after the announcement of the joint start up of Kurz and Hulio)[621]; founder of PayPal and of controversial company Palantir (connected to the Cambridge Analytica scandal); sponsor of

[608] Persons naturalised/registered as citizens of Malta 2017. Published 21 December 2018. https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf
[609] https://mlt.databasesets.com/company-all/company/73006
[610] https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/
[611] https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429
[612] https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=543a981a3997
[613] https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/
[614] https://www.euractiv.com/section/all/short_news/mep-calls-out-malta-for-selling-passport-to-man-linked-to-pegasus-spyware/
[615] https://daphnecaruanagalizia.com/2016/08/owner-israeli-phone-surveillance-hacking-software-intelligence-operation-buys-maltese-passporteu-citizenship/
[616] https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/
[617] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/
[618] https://offshoreleaks.icij.org/nodes/55071906
[619] https://www.haaretz.com/israel-news/tech-news/2022-04-19/ty-article/israeli-predator-spyware-found-in-phone-of-top-greek-investigative-reporter/00000180-6565-dc5d-a1cd-757f069c0000
[620] https://offshoreleaks.icij.org/nodes/55071906
[621] https://www.nytimes.com/2022/10/15/technology/peter-thiel-malta-citizenship.html

Obtenu pour vous par
Got for you by
agence europe

Donald Trump; first outside investor of Facebook; hired Sebastian Kurz (who recently set up business with Shalev Hulio, ex-NSO) as strategist[622];

France

Victims in France

324. In the summer of 2021, the Pegasus Project revealed several cases of attempted hacks by the Pegasus spyware in France.[623] This leaked dataset included the telephone number of President Emmanuel Macron, as well as the phone numbers of 14 members of his cabinet.[624][625] Findings of forensic analyses have confirmed that the telephones of minister of education Jean-Michel Blanquer, minister of territorial cohesion Jacqueline Gourault, minister of agriculture Julien Denormandie, minister of housing Emmanuelle Wargon and minister of overseas Sebastien Lecornu were infected with the Pegasus spyware.[626]

325. The register as seen by the Pegasus Project additionally contained other French citizens as well, amongst them journalists, former politicians and relatives thereof. Pegasus infection of mobile devices belonging to director of Parisian radio station Bruno Delport, former minister Arnaud Montebourg and investigative journalists Edwy Plenel, Lénaïg Bredoux and an unnamed journalist from France 24 have been confirmed.[627] In addition, Claude Mangin - wife of Naâma Asfari, a Sahrawi political prisoner in Morocco - was also targeted with Pegasus.[628] Morocco seems to be behind many of the attacks of both journalists and politicians.[629]

326. Reportedly, France was about to purchase the Pegasus spyware itself in 2021. At the time of the final negotiations with NSO Group, revelations about the spyware allegedly being used against French government officials led to the abrupt suspension of the sale.[630] The French Ministry of Foreign Affairs has denied talks with NSO Group.[631]

Spyware companies in France

327. 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.[632] Nexa Technologies is run by former managers of Amesys. Amesys was founded in 1979[633] 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.[634]

328. In 2007, Amesys reportedly sold this telecommunication surveillance technology to Libya, which has been used by the Gaddafi regime to arrest and torture critics of the regime.

[622] https://www.politico.eu/article/austria-former-chancellor-sebastian-kurz-palantir-technologies-silicon-valley-peter-thiel/
[623] The Guardian. Pegasus spyware found on journalists' phones, French intelligence confirms.
[624] The Guardian. Spyware 'found on phones of five French cabinet members'.
[625] Euractiv. France's Macron targeted in project Pegasus spyware case.
[626] The Guardian. Spyware 'found on phones of five French cabinet members'.
[627] Haaretz. The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.
[628] Haaretz. The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.
[629] RadioFrance. Projet Pegasus : le gouvernement et toute la classe politique française dans le viseur du Maroc.
[630] MIT Technology Review. NSO was about to sell hacking tools to France. Now it's in crisis.
[631] MIT Technology Review. NSO was about to sell hacking tools to France. Now it's in crisis.
[632] Bloomberg. Nexa Technologies Inc.
[633] PitchBook. Amesys.
[634] Le Monde. Vente de matériel de cybersurveillance à l'Egypte : la société Nexa Technologies mise en examen

Obtenu pour vous par
Got for you by
agence europe

According to Telerama, Nexa was founded to rebrand the surveillance software and to continue the sales of Amesys to the Egyptian regime.[635] In 2014, Nexa technologies had allegedly sold an interception system to the Egyptian regime under the name Eagle. This system was used in connection with the detention and torture of political opponents of the Al-Sissi regime[636]. Eagle was deployed and maintained by Amesys from 2007 until 2011.[637]

329. Several complaints have been filed against both Amesys and Nexa Technologies. In October 2011, the FIDH and LDH filed a lawsuit against Amesys at the Paris High Court in light of their alleged sales to Libya.[638] Five Libyan victims were heard in the summer of 2013 and one Libyan victim was heard in December 2015. Due to new evidence underlining the use of Amesys' surveillance technology by the Gaddafi regime, Amesys was officially marked assisted witness for complicity in torture between 2007 and 2011.[639]

330. In 2010, Amesys was taken over by French computer firm Bull. In 2014, Atos, led at the time by Thierry Breton, took over Bull, and thus equally acquired Amesys.[640] At the time of the take over, the dubious activities of Amesys were already well known, indeed a complaint had already been lodged.

331. In 2017, an investigative media report revealed the sale of surveillance systems to Egypt in 2014, triggering a complaint by FIDH, LDH and Cairo Institute for Human Rights Studies (CIHRS).[641] This lawsuit was filed against Nexa technologies.[642]

332. Following several complaints by human rights organisations, in June 2021 the Paris Judicial Court indicted four executives of Amesys and Nexa Technologies over the sale of surveillance technology to the governments in Libya and Egypt.[643] It is worrying that no less than ten years have passed between the first complaint and the start of the court case. Meanwhile Amesys has been able to continue its activity unhampered, including the above-mentioned sale of surveillance technology to Egypt.

333. Despite these controversies, the French d'Agence Nationale des Titres Sécurisés (ANTS) signed a contract with Amesys in October 2016 worth over 5 million euros for the technical management of the TES database (containing personal data and biometrics of all French citizens). This decision of the French authorities to involve Amesys, then already known for its practices, in such a project was subject to criticism. Whilst Amesys would not be in full control of the systems used for the controversial TES database file, it would assist the agencies project managers who deal with the TES file, so it cannot be excluded that Amesys would have access to personal data. However, the Director of ANTS considered that there was no legal objection to conducting business with Amesys.[644]

[635] ZDNet. Amesys and Nexa Technologies executives indicted.
[636] Trial International. Amesys (Nexa Technologies).
[637] ZDNet. Amesys and Nexa Technologies executives indicted.
[638] Trial International. Amesys (Nexa Technologies).
[639] Trial International. Amesys (Nexa Technologies).
[640] L'Obs. Amesys file un coup de main à l'agence en charge du fichier monstre.
[641] Le Monde. Vente de matériel de cybersurveillance à l'Egypte : la société Nexa Technologies mise en examen
[642] ZDNet. Amesys and Nexa Technologies executives indicted.
[643] Amensty Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture.
[644] L'Obs. Amesys file un coup de main à l'agence en charge du fichier monstre.

Obtenu pour vous par
Got for you by
agence europe

334. In France, the provision of export licenses is controlled by the Dual-Use Goods Service (SBDU) of the Ministry of Economy, Industry and Digital Affairs. In addition, the Inter-Ministerial Commission on Dual-Use items - chaired by the Ministry for Europe and Foreign Affairs - inspects the more sensitive dual use items. At the time of writing, there is no information on the facilitation of export licenses by the French government to Nexa Technologies.

Ireland

335. 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.[645]

336. Published accounts by Thalestris for the period ending on 31 December 2020 indicate that there are 10 other subsidiary companies in Greece, Cyprus, Switzerland, and the British Virgin Islands, and that Thalestris was not liable to pay any corporation tax. It used a number of fiscal provisions also used by multinationals operating in Ireland, and was therefore technically loss-making.[646]

337. The Irish government refused to respond to the question on whether it or law enforcement agencies had been approached by Thalestris or Intellexa, or if they ever used their services: *"For sound operational and national security reasons it would not be appropriate to comment on the details of national security arrangements, nor would it be appropriate to disclose the department's cyber security arrangements or those of state offices, agencies and bodies under the department's remit."* The Irish government also refused to comment on any Irish links of the spyware produced by Thalestris and Intellexa.[647]

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

Obtenu pour vous par
Got for you by
agence europe

338. Haaretz revealed that a firm called GoNet Systems, which was involved in providing Wi-Fi infrastructure services at Larnaca Airport, and which was linked to Dilian's WiSpear and shut down in 2022, also had corporate ownership in Ireland.[648]

Luxemburg

339. Luxemburg hosts nine entities directly related to NSO Group, as was revealed by Amnesty International in June 2021.[649] The fact that Foreign Minister Jean Asselborn was initially only aware of two NSO entities based in the country[650], 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.

340. Following the Amnesty revelations about the existence of nine NSO entities in Luxemburg in June 2021, all under the umbrella of management and private equity firm Novalpina Capital, Asselborn sent each of them a letter about their legal obligations and human rights duties. According to LuxTimes, NSO Group replied that it only exports its spyware from Israel with the consent of the Israeli government, but Asselborn stated in October 2021 that he could not verify that.[651] In any case, according to the minister, none of the nine entities was authorised to export cyber-surveillance products from Luxemburg, as Luxemburg has not granted any export licence.[652] *"Luxembourg will not, under any circumstances, tolerate that export operations from Luxembourg contribute to human rights violations in third countries and will ensure, if applicable, to take the necessary measures to remedy any violation of human rights and to prevent future violations"*, said Asselborn.[653] However, NSO Group is still able to operate thanks to the entities based in Luxemburg, such as Q Cyber Technologies, which is responsible for handling invoices, contracts and payments from customers of its software.[654] On 24 August 2022, it was revealed that NSO Group booked more than half of its sales over the two previous years in Luxemburg, making clear that Luxemburg functions as an important business hub for NSO Group.[655]

[648] https://www.haaretz.com/israel-news/security-aviation/2022-09-20/ty-article-magazine/.highlight/as-israel-reins-in-its-cyberarms-industry-an-ex-intel-officer-is-building-a-new-empire/00000183-5a07-dd63-adb3-da173af40000?lts=1667755247674
[649] https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[650] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e
[651] https://www.luxtimes.lu/en/luxembourg/government-cannot-verify-pegasus-export-claims-616eead9de135b9236b1efcc
[652] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e
[653] https://delano.lu/article/nine-nso-entities-in-luxembour
[654] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e
[655] https://www.luxtimes.lu/en/business-finance/pegasus-firm-nso-booked-most-sales-through-luxembourg-6303754ade135b9236e0870b

Obtenu pour vous par
Got for you by
agence europe

341. In October 2021, Prime Minister Xavier Bettel has confirmed that Luxemburg bought and used Pegasus, "for reasons of state security".[656]

Italy

342. 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.[657] 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.

343. However, two spyware companies, Tykelab and RCS Lab, have chosen Italy as their base for business. More information on these companies can be found in the chapter on the spyware industry.

Austria

344. 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.[658] 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.

345. Kurz resigned from office in October 2021 following a string of scandals. He withdrew from politics in December of the same year. He was subsequently hired as global strategist for Thiel Capital, owned by billionaire Peter Thiel.[659] In October 2022 Sebastian Kurz and Shalev Hulio (founder of NSO Group) launched a cyber security firm called Dream Security.[660] Although Hulio had stepped down as NSO Group CEO in August 2022, Dream Security and NSO have close ties through various personalities and business connections. One of its investors, Adi Shalev, was also an early investor in NSO. Gil Dolev is another founding member of Dream Security. Dolev's sister Shiri Dolev is the President of NSO Group. Shalev Hulio has previously acquired one of Gil Dolev's companies.[661]

346. A company in Austria that has recently become subject of criminal proceedings by the Austrian Ministry of Justice is DSIRF GmbH (LLC)[662], an Austrian company based in Vienna

[656] https://www.luxtimes.lu/en/luxembourg/tax-voting-rights-housing-watch-bettel-video-highlights-6176e835de135b923682378d
[657] https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/
[658] Responses by former Minister of Interior Karl Nehammer to Member of National Council Nikolaus Scherak, 22 September 2021, Reference 2021-0.580.421
[659] https://www.bloomberg.com/news/articles/2021-12-30/billionaire-thiel-gives-austria-s-former-wunderkind-a-job
[660] https://www.spiegel.de/netzwelt/web/sebastian-kurz-und-ex-nso-chef-gruenden-it-sicherheitsfirma-dream-security-a-4482132c-9faf-4be3-927a-86560ba28670
[661] https://www.timesofisrael.com/former-nso-ceo-ex-chancellor-of-austria-establish-new-cybersecurity-startup/
[662] DSIRF is an abbreviation for "Decision Supporting Information Research and Forensic"

Obtenu pour vous par
Got for you by
agence europe

with a parent company in Liechtenstein that was founded in 2016. More information on DSIRF is provided in the Chapter on the Spyware industry.

Estonia

347. 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.[663]

348. However, one year later, a Russian defence official notified Israel on the Estonian intention to use the Pegasus spyware on Russian phone numbers. This information led the Israeli ministry of Defence to block Estonia from spying on any Russian devices worldwide, stating that the deal would be harmful to Israeli-Russian relations.[664] The case of Estonia underlines that the Pegasus spyware is not just a surveillance weapon, but also political currency in diplomatic relations.

Lithuania

349. 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".[665] He also acquired a Maltese golden passport in 2015. [666]

Bulgaria

350. 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.[667] The current minister of Economy and Industry is Nikola Stoyanov.[668] Up until today, the Bulgarian authorities deny having granted export licenses to NSO Group.[669] Yet, former private equity owner of NSO Group

[663] The New York Times. Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia
[664] The New York Times. Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia.
[665] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/
[666] https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429
[667] Republic of Bulgaria. Ministry of Economy and Industry. Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction.
[668] Council of Ministers of the Republic of Bulgaria.
[669] POLITICO. Pegasus makers face EU grilling. Here's what to ask them.

Obtenu pour vous par
Got for you by
agence europe

Novalpina Capital emphasised that NSO products are being exported from the EU from both Cyprus and Bulgaria.[670][671][672]. These two claims are contradictory.

351. As outlined in the chapter on Cyprus, Tal Dilian's company Circles Technologies was sold to former private equity firm Francisco Partners and later on it was merged with NSO Group.[673] NSO Group has several subsidiaries registered in Israel, the UK, Luxembourg, the USA, Cyprus and Bulgaria. The Bulgarian subsidiaries of NSO Group provide the Cypriot subsidiaries of research and developments services and export network products to governments.[674]

352. As of April 2014, a subsidiary under the name of Magnet Bulgaria EOOD was launched in Sofia with the Cypriot MS Magnet Solutions Ltd. as parent company. The main business activities of Magnet Bulgaria are "Development and distribution of software and hardware; consultancy and product development for private, governmental and non-governmental organisations in the field of computer technology and software and telecommunications; integration of software and telecommunications products; marketing and management; information services; internal and external trade; transport and forwarding activities in the country and abroad; participation in other commercial companies; transactions with intellectual property rights; real estate transactions; rental; and all other activities not prohibited by law."[675][676].

353. In July 2017, Circles Bulgaria EOOD - another NSO subsidiary - registered in Sofia with the Cypriot CS-Circles Solutions Ltd. as parent company. The main activities of Circles Bulgaria are described as 'Computer Systems Design and Related Services'. The company employs 147 people at the time of writing.[677]

354. According to the Public Register of Persons Registered for Export and Transfer of Dual-Use Items and Technologies as provided for by the Bulgarian Ministry of Economy, both NSO subsidiaries Magnet Bulgaria and Circles Bulgaria have received export licenses. Magnet Bulgaria received an export license that expired on 12 May 2020.[678] Based on a letter sent by NSO to Amnesty International, Magnet Bulgaria is dormant at time of writing.[679] Circles Bulgaria is currently still active and has received an export license that is valid until 25 April 2023.[680] Whereas NSO Group subsidiaries have received export licenses from the Bulgarian authorities, the Bulgarian government denies the granting of export licenses to

[670] Amnesty International. Novalpina Capital's response to NGO coalition's open letter (18 February 2019).
[671] Access Now. Is NSO Group's infamous Pegasus spyware being traded through the EU?
[672] https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/
[673] Joe Galvin. An address in north Dublin, 20m in spyware sales and no tax: Inside the Predator's Irish lair.
[674] Amnesty International. Operating From the Shadows: Inside NSO Group's Corporate Structure.
[675] Amnesty International. Operating From the Shadows: Inside NSO Group's Corporate Structure.
[676] Opencorporates. Magnet Bulgaria ltd.
[677] EMIS. Circles Bulgaria EOOD.
[678]https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuseruploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK
[679] Amnesty International. Operating From the Shadows: Inside NSO Group's Corporate Structure.
[680]https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuseruploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK

Obtenu pour vous par
Got for you by
agence europe

NSO group itself.[681]

355. The Sofia City Prosecutor's Office has started an investigation to inquire if the Pegasus Spyware has been illegally used by Bulgarian government entities. This inquiry is ongoing at the time of writing.[682][683]

[681] Access Now. Is NSO Group's infamous Pegasus spyware being traded through the EU?
[682] BNR. Sofia City Prosecutor's Office investigates possible use of Pegasus spyware in Bulgaria.
[683] European Parliament. Pegasus and surveillance spyware.

Obtenu pour vous par
Got for you by
agence europe

I.G. EU Institutions

Targeting of the European Commission

356. 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".[684] 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.[685] 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.[686]

357. According to the Commission's response to the PEGA committee on 9 September 2022[687], these checks did not confirm any compromise of Commissioner Reynders's personal or professional device, "neither ... before or after this date [23 November]". The Commission's competent services also inspected devices of additional staff who received similar notifications from Apple on the same day, but "none of the inspected devices confirmed Apple's suspicions" either.

358. However, in letters of 25 July 2022 and 9 September 2022, the Commission acknowledged that in the course of the ongoing investigation into the targeting of the Commission with Pegasus, "several device checks led to the discovery of indicators of compromise." The Commission has so far refused to further elaborate on the investigation's findings, as "they would reveal to adversaries the Commission's investigation methods and capabilities, thus seriously jeopardizing the institution's security." [688][689] Unofficial reports of some sixty detected infections have not been confirmed by the Commission.

359. On 15 July 2022 the PEGA committee asked the Commission whether it requested the assistance of Citizen Lab for its investigation. However, the Commission did not deem it necessary to follow up further, and stated that "the information made publicly available by Citizens Lab and Amnesty International did not allow to confirm that Commissioner Reynders's devices were infected by Pegasus"[690], despite the fact that compromise was found on "several devices".

360. The Commission has declared that "Notifications of this kind are received multiple times on any given day by the Commission's relevant IT departments" and therefore they do not merit to be officially reported to the police. According to the Commission, since the Apple notification did not signal a "definitive infection, but the possibility of an attempt by the

[684] Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022
[685] 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
[686] https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/
[687] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022
[688] Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022
[689] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022
[690] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

Obtenu pour vous par
Got for you by
agence europe

malware to target the corresponding device", the Commission did not follow up with law enforcement authorities.[691] However, in contrast to the usual practice of non reporting, the Commission states that it "has been in contact with the Belgian police", on "technical details", as part of its "regular cooperation". It does not seem that the Commission officially reported the notifications or the "indicators of compromise" to the Belgian police for further investigation.[692] This is remarkable. In other cases, for example Spain and France, a criminal investigation has been launched into the use of spyware against government ministers and heads of state. Spyware is used mainly by state actors, for reasons of national security. The Commission argues that "some aspects linked to national security fall outside the competences of the Commission", but it fails to explain how Commissioners and Commission staff would plausibly constitute a risk to national security.

361. 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[693], 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."[694]

362. 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

363. 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. This solution would help the Commission's services to "identify potentially infected corporate mobile devices. Whenever there are indications of infections, a security review of the device is organised." The Commission says to cooperate continuously with CERT-EU, the Computer Emergency Response Team of the Union's institutions, bodies, and agencies, and to issue recommendations and guidance to CERT-EU's constituents.[695]

Targeting of former Greek Commissioner and representatives in the Council

364. 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

[691] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022
[692] Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022
[693] https://pro.politico.eu/news/148627
[694] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022
[695] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

Obtenu pour vous par
Got for you by
agence europe

Avramopoulos, European Commissioner from 2014-2019 and Néa Dimokratía politician.[696] 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 many politicians from both Néa Dimokratía and opposition, the most plausible hypothesis is that the orders came from the entourage of the Prime Minister.

365. 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.

[696] Documento, edition 6 November 2022.

Obtenu pour vous par
Got for you by
agence europe

II. The Spyware industry

366. 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.[697][698] Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.

367. The spyware industry has a spaghetti-like structure: complex, opaque and elusive. Whoever tries to map out the sector will get lost in an impenetrable maze of persons, locations, connections, ownership structures, letterbox companies, ever changing corporate names, money flows, government proxies and middlemen, tycoons and governments. This seems to be a strategy of deliberate "corporate obfuscation".

368. 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.[699] 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.

[697] Makarios Drousiotis. State Mafia. Chapter 6. Published 2022
[698] Haaretz. Cyprus, Cyberspies and the Dark Side of Israeli Intel.
[699] 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

Obtenu pour vous par
Got for you by
agence europe

369. Next to the "official channels" there is also a black market for these products. Although many vendors claim they only sell to governments, it would seem they secretly also try to do business with non-state actors. It is very difficult to find waterproof evidence, as by definition this trade shuns daylight and leaves no traces. Greek newspaper Documento claims to have evidence that the software is being sold on the black market – for up to $50 million – not only to governments and counter-terrorism agencies, but also to private individuals.[700] Another Greek newspaper, To Vima, reported that Predator was sold to 34 customers from Greece.[701] Given that spyware is illegal in Greece, that is a stunning number. Leaked documents show a pirated version of the product that was officially sold only to governments, at a price of $8 million, an amount that included training the agents who will use the program, 24-hour technical support and monitoring of the victim's social media accounts.[702]

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

Vulnerabilities

371. 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.[703] 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.

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

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

[700] Documento. Documento's 'Predator' revelations on Euractiv – Europol's intervention calls for Dutch MEP
[701] To Vima. Interceptions “Spy software has 34 customers.”
[702] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/
[703] Ot van Daalen, intervention in PEGA 27 October 2022;
EDRi Paper: Breaking encryption will doom our freedoms and rightshttps://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

Obtenu pour vous par
Got for you by
agence europe

Telecom networks

374. 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).[704] 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.[705]

375. The risk of abuse by the telecom providers of access to these networks is high. We have several documented misuses, where access points (global titles) where leased to shady companies that were monitoring and intercepting communications of targets based on the man in the middle attacks. They were also harvesting geo-location data, meta-data for their own economical purposes. A global title is an address used for routing messages within Signaling System Number 7 (SS7). It can be compared to an IP address, in that the global title refers to an address within the telecommunications system.[706] This is also the reason why the access to the SS7 network in US was so interesting for NSO, that they were trying to buy their access with "bags of cash".[707] Telecom providers are deliberately keeping these low industry standards in order to provide an easier access to local state enforcement agencies.

376. The remainder of this chapter outlines the most prominent actors of the spyware industry in Europe: NSO Group, Intellexa Alliance, Candiru, Tykelab and RCS Lab, DSIRF, and the former FinFisher.

NSO Group

377. 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.[708] Pegasus spyware is the best known product of NSO Group. It was brought onto the global market in 2011.[709][710]

378. Since its launch in 2010, NSO Group has had corporate presence in Israel, the UK, Luxembourg, the Cayman Islands, Cyprus, the US, the Netherlands, Bulgaria and the British Virgin Islands. A lot of information regarding the roles of the different corporate entities is

[704] https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7 was first adopted as,up to and including 5G
[705] https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/
[706] https://www.gms-worldwide.com/glossary/global-title/
[707] https://www.theguardian.com/news/2022/feb/01/nso-offered-us-mobile-security-firm-bags-of-cash-whistleblower-claims
[708] NSO Group. About us.
[709] NYTimes. The Battle for the World's Most Powerful Cyberweapon.
[710] Hulio S., NSO Never Engaged in Illegal Mass Surveillance, The Wall Street Journal, 24 February 2022

Obtenu pour vous par
Got for you by
agence europe

still lacking and some of these companies have already been liquidated. NSO Group has however stated in their Transparency and Responsibility report of 2021 that Bulgaria and Cyprus are both export hubs.[711] According to Amnesty International, the Dutch entities (liquidated on December 22, 2016) functioned in the sector of financial holdings and Q Cyber Technologies as based in Luxembourg was active as a commercial distributor responsible for the issuance of invoices, signing of contracts and receiving payments from customers. In addition, Westbridge Technologies as registered in the US may have facilitated the company's US sales.[712]

379. NSO reportedly had revenues of $243 million in 2020.[713] However, following the revelations by the Pegasus Project, the company faced several difficulties. Lawsuits filed by Apple[714] and Meta[715] against the company, blacklisting of NSO by the US Commerce department, the tightening of the Israeli export regime, critical inquiries in several countries, and internal frictions within the private equity fund behind NSO group, have led to a severe decline in profit. Reportedly, NSO Group's debt at one point even reached 6.5 times its normal revenues for a year.[716]

380. Pegasus spyware was initially sold to twenty-two end-users in fourteen EU Member States, using marketing and export licenses issued by Israel. Contracts with end-users in two Member States were subsequently terminated.[717] It has not been confirmed which Member States are included in the list of fourteen, nor which two countries were removed. However, it is generally assumed the two are Poland and Hungary.

Corporate structure, transparency and due diligence

381. On January 25 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.[718]

382. In March 2014, private equity fund Francisco Partners obtained a 70% stake in NSO Group. Under Francisco Partners, the company expanded its entities to different jurisdictions, including Cyprus, Bulgaria, the USA, the Netherlands and Luxembourg. During the Francisco Partners years between 2014 and 2019, the fund systematically reviewed the sale of NSO Group's products through the Business Ethics Committee (BEC). According to

[711] NSO Group. Transparency and Responsibility Report 2021.
[712] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.
[713] Haaretz. NSO Is Having a Bad Year - and It's Showing.
[714] Apple. Apple sues NSO Group to curb the abuse of state-sponsored spyware.
[715] Bloomberg Law. NSO Loses Latest Challenge to Meta Lawsuit Over Whatsapp Spyware.
[716] Bloomberg. Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop.
[717] Answers provided by NSO Group to PEGA secretariat following hearing, 20 July 2022. z
[718] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

Obtenu pour vous par
Got for you by
agence europe

Francisco Partners, the BEC has denied tens of millions of dollars' worth of sales that would have otherwise be approved of under legal requirements.[719]

383. Francisco Partners sold their entire ownership interest, including that of the subsidiaries, on February 14, 2019 to Novalpina Capital. With this management buyout, the governance standards changed and the BEC was replaced by the Governance, Risk and Compliance Committee (GRCC) for the review of human rights records of potential customers.[720]

384. In line with the End Use/User Certificate after the tightening of the Israeli export regime, NSO Group has introduced a Human Rights Policy and a Human Rights Due Diligence (HRDD) procedure. As described in NSO Group's Transparency and Responsibility report of 2021, NSO group requires that all customer agreements include human rights compliance clauses and clauses outlining the suspension or termination of the use of NSO Group's products in case of human rights-related misuse. In a written submission to PEGA, NSO Group confirmed that it has terminated contracts with EU Member States[721], supposedly breaching the human rights clauses. Although it is not confirmed, it is assumed this decision concerns Poland and Hungary. NSO Group has not clarified if it has done an examination of the audit logs, and whether the customers in question had consented to such an examination. It is therefore not known if any evidence of the abuse still exists, if NSO has any way of preserving that evidence or if the Israeli authorities have any evidence.

385. According to Amnesty International, the transparency report of NSO Group lacks a proper remediation policy for victims of unlawful surveillance and information on the ongoing lawsuits against NSO Group is absent.[722] It becomes clear that NSO Group hides behind its Human Rights Policy and HRDD procedure as it spyware continues to be detected on devices of journalists and critics of authoritarian regimes.[723] The reality tells the true story, not the corporate policies.

Export Controls

386. 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.[724] Most of these licenses are granted by the Israeli authorities.[725] 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.[726] The Ministry of Defence's (MOD) Defence Export Control Agency (DECA) is responsible for the issuance of marketing and export licenses.[727] Following the Pegasus Project revelations and the blacklisting of NSO,

[719] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.
[720] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.
[721] PEGA Committee Hearing with NSO, 21 June 2022;
[722] Amnesty International, NSO Group's new transparency report is 'another missed opportunity', press release, 1 July 2021
[723] NYTimes. U.S. Blacklists Israeli Firm NSO Group Over Spyware.
[724] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure. P. 62.
[725] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.
[726] European Parliamentary Research Service. Europe's PegasusGate. Countering spyware abuse.
[727] Amnesty International. Novalpina Capital's reply to NGO coalition letter (15 April 2019) and Citizen Lab letter (06 March 2019)

Obtenu pour vous par
Got for you by
agence europe

the list of eligible countries has been reduced from 102 down to 37, which all need to sign an End Use/User Certificate.[728] 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.

387. NSO Group has confirmed that it exports its products from Bulgaria and Cyprus, but denies the export of the Pegasus spyware from these two countries in particular.[729] Cyprus and Bulgaria have in addition denied having granted any export permits to NSO companies in general. As described in the chapters on Cyprus and Bulgaria, NSO subsidiaries often hide behind a different name in the national business registers. One of NSO's subsidiaries in Cyprus under the name of Circles has however closed its offices in 2020.[730]

Unethical behaviour triggering lawsuits, blacklisting and investor conflicts

388. 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.[731] On August 27, 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.[732] 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.[733] On April 25, 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.[734] The Luxembourg court has dismissed these demands and BRG remains in charge of the fund controlling NSO Group.[735]

389. In addition to ownership fall-outs, the US Commerce Department placed NSO Group on 3 November 2021 on a blacklist due to the incompatibility of NSO's activities with US foreign policy and national security concerns. The US administration prohibits the export of technology to NSO Group and its subsidiaries, de facto meaning that no American company can work with NSO Group.[736]
390. In response to the US Blacklisting, Credit Suisse, as one of the creditors of NSO Group, allegedly pushed the company to continue its sales of the Pegasus spyware to new customers. In a letter to BRG sent by Willkie Farr & Gallagher, several creditors stated that they were concerned that BRG was preventing NSO Group "from pursuing and obtaining

[728] European Parliamentary Research Service. Europe's PegasusGate. Countering spyware abuse.
[729] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.
[730] VICE. NSO Group Closes Cyprus Office of Spy Firm.
[731] Financial Times. Private equity owner of spyware group NSO stripped of control of €1bn fund.
[732] Financial Times. NSO Group keeping owners 'in the dark', manager says.
[733] The New Yorker. How democracies spy on their citizens.
[734] Letter to Mr Jeroen Lenaers and his Vice Chairs.
[735] Luxembourg Times. Top five stories you may have missed.
[736] NYTimes. U.S. Blacklists Israeli Firm NSO Group Over Spyware.

Obtenu pour vous par
Got for you by
agence europe

new customers". One of the creditors - although not named in the letter - seems to be Credit Suisse. BRG responded to the lenders that it was deeply concerned about the pressing for NSO Group sales.[737]

391. A few days after the US blacklisting of NSO, the United States Court of Appeals confirmed the proceeding of Meta's lawsuit against NSO, immediately followed by a complaint lodged at the federal court by Apple.[738] In June 2022, the United States District Court rejected NSO Group's claim to immunity in the Apple lawsuit.[739] At time of writing, the Apple lawsuit against NSO Group is still pending.

392. Around June 2022, a US defence contractor under the name of L3Harris was reportedly negotiating a deal with the NSO Group to take over NSO Groups 'surveillance technology behind the Pegasus product as well as its personnel. Such a potential deal would have required the approval from both the US and Israeli government[740] and had to meet the US Intelligence Services condition of selling Pegasus' software vulnerabilities and source code to the Five Eyes.[741] According to a White House official, the deal would spur counterintelligence concerns and would not necessarily withdraw the company from the US blacklist.[742] Due to such security concerns by the Biden administration, L3Harris terminated its negotiations in July 2022.[743]

393. Despite of the US blacklisting, the Biden administration has allegedly appointed a former NSO advisor to an intelligence advisory board in October 2022. His name is Jeremy Bash. Under the auspices of Beacon Global Strategies, Bash was reportedly hired to advice NSO Group through Francisco Partners. According to the Guardian, he was one of the eight members on NSO's business ethics committee, allegedly providing him with a vote on the proceedings of proposed NSO sales. Beacon Global Strategies terminated the work with NSO after the pursued sales to Saudi Arabia.[744]

394. NSO Group has similarly suffered from departing personnel. Since the murder on Jamal Khashoggi and the growing concerns of the role of Pegasus therein, many employees have left NSO Group. Following these departures, Mr Hulio responded, "What worries me is the vibes of the employees."[745] In August 2022, NSO Group announced to fire 100 employees.[746] That same month, co-founder Shalev Hulio stepped down as CEO of NSO

[737] Financial Times. Credit Suisse pushed for spyware sales at NSO despite US blacklisting.
[738] NYTimes. Apple Sues Israeli Spyware Maker, Seeking to Block Its Acces to iPhones.
[739] https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/35/
[740] The Guardian. US defence contractor in talks to take over NSO Group's hacking technology.
[741] The Washington Post. American firm drops bid for Israeli spyware following U.S. concerns.
[742] The Guardian. US defence contractor in talks to take over NSO Group's hacking technology.
[743] The Washington Post. American firm drops bid for Israeli spyware following U.S. concerns.
[744] The Guardian. Biden intelligence advisor previously vetted deals for Israeli NSO Group.
[745] The New Yorker. How Democracies spy on their citizens.
[746] Calcalist. After cutbacks and CEO departure, what's next for the controversial NSO?

Obtenu pour vous par
Got for you by
agence europe

Group and was replaced by Yaron Shohat.[747] [748] NSO group changed policy and now focuses only on NATO members.[749]

395. In October 2022, Shalev Hulio and former Chancellor of Austria Sebastian Kurz launched a new cybersecurity firm called "Dream Security". Mr Kurz stepped down as chancellor after a corruption scandal in October 2021 and started working for Peter Thiel's investment firm two months later. The company will produce solutions in the field of cyber incidents, centring on artificial intelligence, and will focus its sales on the European market.[750][751]. The cooperation between Kurz and Hulio constitutes an indirect but alarming connection between the spyware industry and Peter Thiel and his firm Palantir.

396. Gil Dolev is a founding member of Dream Security. Gil Dolev is the brother of Shiri Dolev, NSO Group President. Gil Dolev also founded Wayout Group, a company specialised in intelligence gathering.[752] Dream Security already raised $20 million from several investors, like Adi Shalev who was also involved in NSO investments. Other investors include Yevgeny Dibrov[753], who represents 'the New Russian voice in what he calls 'the Russian-Israeli tech ecosystem'.[754]

Black Cube

397. Black Cube is an Israeli private intelligence agency comprised of former employees of Mossad, the Israeli military and Israeli intelligence services.[755] Their own company website dubs them as a "creative intelligence service" finding "tailored solutions to complex business and litigation challenges".[756] Black Cube have been involved in a number of public hacking controversies including in the US and Romania.[757] More particularly, the heads of Black Cube admitted spying on the former chief prosecutor of Romania's National Anti-Corruption Directorate Laura Kovesi.[758] 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.[759]

398. 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

[747] The Washington Post. CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup.
[748] Calcalist. After cutbacks and CEO departure, what's next for the controversial NSO?
[749] The Guardian. CEO of Israeli Pegasus spyware firm NSO to step down.
[750] OCCRP. Former Austrian Chancellor and ex-NSO Chief Start Cybersecurity Firm.
[751] The Times. Former NSO CEO and ex-Austrian Chancellor found startup.
[752] The Times of Israel. Former NSO CEO and ex-chancellor of Austria establish new cybersecurity startup.
[753] The Times. Former NSO CEO and ex-Austrian Chancellor found startup.
[754] Calcalist. From Russia, With Coding Skills.
[755] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators , 7 October 2019.
[756] https://www.blackcube.com/
[757] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , 18 April 2022.
[758] Balkan Insight. Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case.
[759] Haaretz. Black Cube CEO Suspected of Running Crime Organisation. Revealed: The Romania Interrogation.

Obtenu pour vous par
Got for you by
agence europe

opponents, former NSO CEO Shalev Hulio admitted to hiring Black Cube at in at least one situation in Cyprus.

399. Black Cube got involved in Hungary during the 2018 elections, during which time they spied upon various NGOs and persons who had any connection to George Soros and reported back to Orban in order for him to spin their actives in a smear campaign.[760] The resulting information from the surveillance of those individuals and NGOs appeared not only in the Hungarian state-controlled media, but also in the Jerusalem Post.[761]

Intellexa Alliance

400. 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 carreer as "intelligence expert, community builder and serial entrepreneur".[762] 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

401. All these vendors facilitate different systems. Whereas Cytrox is skilled in the extraction of data from mobile phones, Nexa technologies offers exploitation of global mobile communication systems. WiSpear can additionally extract data from Wi-Fi networks. The different vendors under Dilian's alliance thus allow for a broad assortment of software and services that Intellexa can offer and combine to its clients within and outside of the EU.[763]

402. Parent company of Intellexa Alliance - Thalestris Limited - has different subsidiaries that have corporate presence throughout Ireland, Greece, the British Virgin Islands, Switzerland and Cyprus. Sara Aleksandra Hamou, reportedly the second ex-wife of Tal Dilian, has been the director of Thalestris Limited, and managing director of a subsidiary based in Greece.[764] Hamou, originally born in Poland, holds a Cypriot passport issued by the Embassy of Poland in Cyprus.[765]

WiSpear and Cytrox

[760] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/ 6 July 2018.
[761] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/ 6 July 2018.
[762] Tal Dilian. About.
[763] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[764] Thalestris Limited. Annual Report and Consolidated Financial Statements for the period from 28 November 2019 to 31 December 2020.
[765] ReportersUnited. The Great Nephew and Big Brother.

Obtenu pour vous par
Got for you by
agence europe

403. 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.[766] 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.[767] Public scandals relating to these products triggered the move of Intellexa's main business activities from Cyprus to Greece.

404. In 2017, Cytrox Holdings Zrt. was founded in North Macedonia by Ivo Malinkovski. However, the cradle of Cytrox was actually in Tel Aviv, and Malinkovski was just the front man. After the Pegasus Project revelations, Malinkovski tried to erase all traces connecting him to Cytrox. (Unsuccessfully, as he left a picture of himself holding a coffee mug with "Cytrox" on it). There were rumours that the person actually in charge is Ivo's father Ilija Malinkovski. Today he owns a restaurant and wine chateau, but since the 1990s he also has a company selling weapons[768], which is interestingly also mentioned on the website of the Greek ministry of Foreign Affairs.[769]

405. Cytrox was the developer of the Predator spyware. In contrast to Pegasus spyware, Predator requires the target to click on a link to install the software.[770] When Cytrox was on the verge of bankruptcy, Tal Dilian rescued it with the acquisition costing under 5 million dollars.[771] Cytrox was subsequently merged with Dilian's WiSpear.[772] This acquisition added the Predator spyware to the arsenal of Intellexa technologies.

406. According to CitizenLab, several Cytrox companies have been registered in Israel - Cytrox EMEA ltd. and Cytrox Software Ltd. - and in Hungary as Cytrox Holdings Zrt.[773] All of the shares of Cytrox Holdings Zrt. and Cytrox EMEA ltd - later renamed to Balinese Ltd. - were transferred to Aliada Group Inc. as registered in the British Virgin Islands. Aliada Group is also the owner of WiSpear. The main shareholders of Aliada Group are Dilian himself, as well as Oz Liv, Meir Shamir and Avi Rubinstein. In December 2020, Rubinstein lodged a complaint against his co-shareholders of Aliada Group for the illegal dilution of his shares. According to the lawsuit, the relocation of shares to the British Virgin Islands and later to Ireland circumvented Israeli and foreign export control laws.[774]

Amesys and Nexa Technologies

[766] Open Corporates. Passitora Ltd. https://opencorporates.com/companies/cy/HE318328
[767] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[768] https://balkaninsight.com/2022/01/06/wine-weapons-and-whatsapp-a-skopje-spyware-scandal/
[769] http://www2.mfa.gr/en/companies/company/1093
[770] European Parliament. Greece's Predatorgate. The latest chapter in Europe's spyware scandal?
[771] BalkanInsight. Wine, Weapons and Whatsapp: A Skopje Spyware Scandal.
[772] Pitchbook. Cytrox overview.
[773] Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.
[774] Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.

Obtenu pour vous par
Got for you by
agence europe

407. Amesys and Nexa Technologies are also part of Intellexa Alliance, and not free from controverse, as mentioned in the Chapter on France.

Poltrex

408. 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[775] 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.[776]

409. When the investigations surrounding Dilian's spyware van were proceeding, the ownership of Alchemycorp Ltd. was transferred to Yaron Levgoren. Levgoren was an employee of Cytrox Holdings.[777] According to his LinkedIn he currently represents the Intellexa company Apollo Technologies, based in Greece.

Candiru

410. 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.[778] Former investor in NSO Group Isaac Zack became the largest shareholder of Candiru. The company sells spyware for the hacking of computers and servers.[779] 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.[780]

411. According to a TheMarker inquiry, Candiru now also offers spyware to break into mobile devices.[781] It solely sells its spyware to governments and its clientele consists of "Europe, the former Soviet Union, the Persian Gulf, Asia and Latin America".[782] As highlighted in the chapter on Spain, four people out of the 65 victims were targeted with Candiru, and at least two people were targeted with both Candiru and Pegasus.[783]

---

[775] Philenews. FILE: The state insulted Avni and Dilian.
[776] CyprusMail. Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.
[777] Philenews. How the spyware scandal in Greece is related to Cyprus.
[778] Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers
[779] Haaretz. Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.
[780] CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.
[781] Haaretz. Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.
[782] CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.
[783] CitizenLab. CatalanGate. Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru.

Obtenu pour vous par
Got for you by
agence europe

412. As with the other spyware vendors, corporate obfuscation lays at the heart of this company, as it has undergone several name changes throughout the last couple of years. The company has changed it names to DF Associates Ltd. in 2017, Grindavik Solutions Ltd in 2018, Taveta Ltd in 2019 and the most recent change to Saito Tech Ltd in 2020.[784] For sake of clarity, we will refer to the company as Candiru.

413. Just like NSO Group, Candiru was similarly placed on the US blacklist by the US Commerce Department in November 2021. It is speculated that the reason for Candiru's blacklisting is the fact that CEO of NSO Group Shalev Hulio allegedly was a secret partner in Candiru and introduced the company to important middlemen in the intelligence world. Reportedly, Mr Hulio would even argue that Candiru's product is actually a repackaging of Pegasus.[785] At a later stage Hulio and Candiru became rivals, as Hulio heard from Francisco Partners that Candiru wanted to compete with NSO Group.[786] On July 1 2022, security researchers identified a novel Chrome zero-day exploit that was used by Candiru to target individuals in Lebanon, Palestine, Yemen and Turkey.[787] The exploit was addressed by Google and has since also been patched by Microsoft and Apple.[788]

Tykelab and RCS Lab

414. 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.[789] In over just two days in June 2022, the company probed networks in almost every country in the world.[790] 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."[791]

415. Lighthouse Report's investigation also highlighted the role of the telecom industry, where the leasing of phone network access points or "global titles" allows for this abuse to continue. According to GSM Association, the industry organisation representing mobile network operators worldwide, phone operators cannot always identify the source and purpose of the traffic that flows through their networks, which makes it difficult to halt these practices.[792]

[784] CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.
[785] Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers
[786] Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers
[787] TechCrunch. Spyware maker Candiru linked to Chrome zero-day targeting journalists.
[788] The HackerNews. Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists.
[789] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[790] https://euobserver.com/digital/155849
[791] http://www.tykelab.it/wp/about/
[792] https://www.lighthousereports.nl/investigation/revealing-europes-nso/

Obtenu pour vous par
Got for you by
agence europe

416. Tykelab is a part of RCS Lab, an Italian company known for its interception activities in Italy and abroad, which was brought to light by an announcement of a third company, Cy4Gate, which acquired RCS Lab. RCS Lab has off-shoots in France, Germany and Spain.[793] RCS Lab has another concealed subsidiary, Azienda Informatica Italiana, which builds interception software for Android and iPhone devices.[794]

Hermit spyware

417. 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 photos.[795] 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[796], and it was also found in Romania.[797]

418. A Threat Intelligence Researcher of cyber security firm Lookout, Justin Albrecht, said that although Hermit's method of installation was less sophisticated than that of Pegasus, its capabilities were similar. Hermit needs a phone user to click on an infected link for it to compromise a device.[798]

419. According to RCS Lab, "any sales or implementation of products is performed only after receiving an official authorisation from the competent national authorities. The products supplied to customers are installed at their facilities, and RCS Lab personnel are not permitted under any circumstances to carry out operational activities in support of the customer or to have access to the processed data. Due to binding confidentiality agreements, RCS Lab cannot disclose any details about its customers. The Cy4gate Group, of which RCS Lab is a member, adheres to the UN Global Compact and therefore condemns all forms of human rights violations. RCS Lab's products are provided with a clear, specific, and exclusive purpose: to support law enforcement agencies in the prevention and suppression of heinous crimes."[799] However, it is not possible to verify if Cy4gate Group, including RCS Lab, adheres to its own declared standards.

DSIRF - Decision Supporting Information Research and Forensic

[793] https://euobserver.com/digital/155849
[794] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[795] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[796] https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

[797] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[798] https://euobserver.com/digital/155849
[799] https://euobserver.com/digital/155849

Obtenu pour vous par
Got for you by
agence europe

420. A company that has recently become subject of criminal proceedings by the Austrian Ministry of Justice is DSIRF GmbH (LLC)[800], 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."[801] DSIRF evidently sells to non-state actors.

421. DSIRF developed spyware called Subzero/KNOTWEED, which can be deployed using zero-day vulnerabilities in Windows and Adobe Reader, and which - according to its own advertising - can be secretly installed on the target device. Once installed, Subzero takes "full control of the target computer" and provides "complete access to all data and passwords". Subzero customers can extract passwords, take screenshots, view current and previous locations, and "access, download, modify and upload files on the target computer" via a web interface. DSIRF promotes Subzero as "next-generation cyber warfare", saying the tool was "designed for the cyber age".[802] In 2020 DSIRF valued its software Subzero with 245 million euros.

422. The connection with Russia become clear from links of several high level staff members of DSIRF. The owner of DSIRF is Peter Dietenberger, a "man with best connections in the Kremlin" and a "door opener of western companies in Putin's empire".[803] Dietenberger lived several years in Russia, had a Russian company and several Russian business partners. One of his Russian business partners, Boris Vasilyev, was also in the board of directors of DSIRF. DSIRF names several references for its firm and products: Michael Harms (CEO of the German Eastern Business Association), Stephan Fanderl (Chairman of the Board of Galeria Karstadt Kaufhof, who wanted to bring Walmart to Russia), Christian Kremer (former President of BMW in Russia and CEO of Russian Machines, which is sanctioned by the US since 2018) and Florian Schneider (partner at the large business law firm Dentons in Moscow)[804]. "Russian Machines", a company owned by the oligarch Oleg Deripaska, is said to be using the services of DSIRF. The powerful local entrepreneur Siegfried "Sigi" Wolf, who advises former Chancellor Sebastian Kurz on economic issues, is considered a confidante of Deripaska[805]. Also Jan Marsalek, an alleged criminal wanted on an Interpol arrest warrant for commercial fraud charges amounting to billions, among other financial and economic offenses, is involved. In August 2018, he received an email from Florian Stermann (Secretary General of the Russian-Austrian Friendship Society, and considered in investigations by the public prosecutor's office to be a "confidant" of the FPÖ)[806] with a company presentation of DSIRF. Already in 2013, he allegedly tried to sell spyware of the Italian company Hacking Team to Grenada. He is said to hide in Moscow at the moment, under the care of the FSB, the

[800] DSIRF is an abbreviation for "Decision Supporting Information Research and Forensic"
[801] https://dsirf.eu/about/
[802] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
[803] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
[804] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
[805] https://www.derstandard.at/story/2000131301583/causa-marsalek-die-verbindungen-einer-spionagefirma-werfen-fragen-auf
[806] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html

Obtenu pour vous par
Got for you by
agence europe

Russian secret service. [807][808] The first office of DSIRF belonged to the then SPÖ chancellor of Austria Christian Kern. Kern and his wife Evelyn Steinberger-Kern bought this loft for one million euros at exactly the time when DSIRF moved in as a tenant.[809]

423. In July 2022, Microsoft found out that Subzero was used during unauthorised, malicious activity to attack law firms, banks, and strategic consultancies in Austria, the United Kingdom and Panama.[810] Austria currently has no legal basis for the unauthorised deployment of spyware like Subzero by public authorities, and it is also illegal if one private company would use it against another. Following the Microsoft publication, on 28 July 2022, the Austrian digital rights NGO Epicenter.works filed a criminal complaint against DSIRF at the Vienna Public Prosecutor's Office for unlawful access to a computer system, data damage, interference with the functioning of computer systems, fraudulent misuse of data processing, criminal organisation and violation of the Foreign Trade and Payments Act with regards to Dual Use Goods.[811] On 7 October 2022, the Austrian Federal Ministry of Labour and Economic Affairs stated that it had not issued an export license to DSIRF[812], and according to the Austrian Federal Ministry for Justice Affairs, the Vienna Public Prosecutor's Office has started a criminal investigation into DSIRF.[813] The use of the Subzero spyware against unknowing targets in Austria means that either a private or public authority in Austria has applied the software illegally, the software was used by a foreign actor and export restrictions were violated by DSIRF or the software was exported to another Member State and used from there legally or illegally against an Austrian target. The investigation is still ongoing.

FinFisher

424. 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[814], including 11 EU Member States[815] and 13 "not-free" countries.[816]

425. In 2017, Finfisher's product FinSpy appeared in Turkey on a fake version of a mobilization website for the Turkish opposition. The software was disguised as a downloadable app

[807] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
[808] https://www.dw.com/en/wanted-wirecard-executive-jan-marsalak-reportedly-hiding-in-moscow/a-61440213
[809] https://www.tagesanzeiger.ch/software-zur-gesichtserkennung-von-shoppern-467623717263
[810] https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/
[811] https://en.epicenter.works/document/4236
[812] Response by Martin Kocher, Federal Minister for Digital and Economic Affairs of Austria, to written parliamentary questions by Stephanie Krisper, 7 October 2022, Reference 2022-0.575.143 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml
[813] Response by Alma Zadić, Federal Minister of Justice, to written parliamentary questions by Stephanie Krisper, 7 October 2022, Reference 2022-0.575.216 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml
[814] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ - https://wikileaks.org/spyfiles4/customers.html
[815] Belgium, Czech Republic, Estonia, Germany, Hungary, Italy, Netherlands, Romania, Slovakia, Slovenia, Spain
[816] Angola, Bahrain, Bangladesh, Egypt, Ethiopia, Gabon, Jordan, Kazakhstan, Myanmar, Oman, Qatar, Saudi Arabia, Turkey

Obtenu pour vous par
Got for you by
agence europe

recommended to participants in anti-government demonstrations.[817] Finfisher itself advertised its products as solely fighting crime. In 2019, a criminal complaint was filed against Finfisher by *Gesellschaft für Freiheitsrechte (GFF)*, *Reporter ohne Grenzen* (RSF Germany), the blog *netzpolitik.org* and the European Center for Constitutional and Human Rights (ECCHR), for exporting its spyware without the necessary export license from the German Federal Office for Economic Affairs and Export Control. It thereby violated the EU Dual-Use Regulation and corresponding German national law. Following the complaint, the Public Prosecutor's Office of Munich investigated FinFisher, and in October 2020 it searched 15 business premises of the FinFisher group of companies in Germany and Romania and private residences. In 2021, the Munich District Court approved the seizure by the Public Prosecutor's Office's of Finfisher's bank accounts, in order to ensure confiscation of illegally obtained profits after FinFisher's possible conviction. However, FinFisher declared insolvency in February 2022. Business operations have ceased, the office has been closed, and all 22 employees were dismissed.[818] The criminal investigations into the people responsible for FinFisher's activities are still ongoing.

[817] https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/

[818] https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/ https://edri.org/our-work/criminal-complaint-against-illegal-export-of-surveillance-software-is-making-an-impact-the-finfisher-group-of-companies-ceases-business-operations-after-its-accounts-are-seized-by-public-prosecutor/ https://netzpolitik.org/wp-upload/2022/03/2022-02-08_AG-Muenchen_Insolvenzbekanntmachung_FinFisher-Labs-GmbH.txt

Obtenu pour vous par
Got for you by
agence europe

III. Legal aspects of the use of spyware in the Union

426. When targeted surveillance, including interception of communications, is used for national security or law enforcement purposes, the use has to comply with applicable Union primary and secondary law.

Charter and Treaty

Fundamental rights

427. Several fundamental rights enshrined in the Charter may be affected by the use of spyware. First of all, such use may interfere with the right to privacy, family life and confidentiality of communications (Article 7). It may also interfere with the right to data protection (Article 8)[819] and the right to freedom of expression guaranteed in Article 11, which constitutes one of the essential foundations of a pluralist, democratic society. The right to property (Article 17) could be affected by the placing of spyware on a targets phone. Furthermore, equality before the law (Article 20) and non-discrimination (Article 21) could be affected, and, the right to a fair trial (Article 47) may also be compromised. Spyware can also have chilling effects on other human rights and fundamental freedoms, including the right to dignity (Article 1), freedom of assembly (Article 12), freedom of religion (Article 11), and even the physical and psychological integrity of an individual (Article 3).

428. Article 52(1) of the Charter lays down the conditions for the limitation of the exercise of fundamental rights. A limitation must be provided for by law[820], respect the essence of the rights and freedoms concerned, be subject to the principle of proportionality[821], and only be imposed if it is necessary (strict necessity[822]) and genuinely meets objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others[823].

429. The CJEU acknowledges that a serious threat to national security that is genuine, present or foreseeable could justify very serious interferences with fundamental rights, subject to strict

[819] The right to data protection is also laid down in Article 16 of the Treaty on the Functioning of the European Union (TFEU), and in Article 39 of the Treaty on the European Union (TEU) and in secondary legislation.
[820] Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, para 175
[821] Judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238
[822] *idem*
[823] Judgment of 15 February 2016, *N.*, C601/15 PPU, EU:C:2016:84, para 50

Obtenu pour vous par
Got for you by
agence europe

conditions and safeguards. Similarly, the prevention of serious crimes, could justify such interference.[824] It should be noted that where a suspicion of such a treat is clearly defined in time, such as with rest of terrorist attacks, it is known when a suspect has been radicalised, the interference cannot encompass data from before the radicalisation.

430. However, the interference must be proportionate given the seriousness of the interference and the importance of the public interest objective pursued[825]. Given the level of interference with the right to privacy, it is highly questionable if spyware such as Pegasus could meet the requirements of proportionality, irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state. [826] This is especially true taking into account that such spyware is not limited to classical wiretapping, as the control over the mobile system allows access not only to incoming/outgoing conversations, but also to all messages, log calls, images and documents on a phone, allowing to build a full profile of a victim through his/her past communications and interactions. Moreover, not only direct victims have their rights affected, but also potentially all their contacts. Therefore, the interference to the right to privacy can be considered even more serious.

Treaty

431. **Article 4 (2) TEU** provides that "*national security remains the sole responsibility of each EU Member State*". That responsibility of Member States corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses "the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities".

432. Secondary law, such as GDPR and the e-Privacy Directive (ePD), goes further as they set out an exclusion for national security. The Law Enforcement Directive (LED) does not apply to activities that falls outside the scope of Union law, but as Article 4(2) TEU is not an exclusion, Union law still applies. In the EU legal order, while national security

[824] Judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, para 156
[825] *idem*, para 131
[826] EDPS Preliminary remarks on Modern Spyware, *edps.europa.eu*, page 8.

Obtenu pour vous par
Got for you by
agence europe

remains the sole responsibility of the Member States, Union law still applies, as confirmed recently by the CJEU[827]. More specifically, a specific rule on national security is applicable only in practices that are purely governmental, without the involvement of any private actor[828]. For clarity, it should be noted that the use of spyware for crime prevention is covered by the e-Privacy Directive and LED.

b. Privacy and data protection law

e-Privacy Directive

433. The ePD seeks to impose obligations on providers of publicly available electronic communications services and requires Member States to adopt laws that guarantee the confidentiality of communications. Article 15 of the ePD allows for restrictions in the form of legislative measures adopted by Member States. These restrictions must however be tailored to specific aims, such as the prevention or detection of crime, and need to meet certain criteria laid down by the ePD and, more generally, EU human rights law, such as necessity and proportionality. This has the effect of bringing national laws within the scope of the ePD and hence EU law, even if the purpose is safeguarding national security (i.e. State security), defence, public security.[829]

434. Since the deployment of spyware does not always require the involvement of providers of electronic communications services, the case law of the CJEU[830] would suggest that the ePD does not apply to the processing of personal data. Where the spyware is actively deployed by the providers or with their assistance, ePD applies.

435. However, the ePD provides in its Article 5 that Member States shall ensure the confidentiality of communications. Article 5(3) of the ePD protects the user's terminal equipment against interference, which also covers smartphone devices. Indeed, this paragraph prohibits not only the storing of information but also the access to already stored information in the user's terminal equipment without the user's consent. Unlike the other provisions of the ePD, the scope of Article 5(3) is not limited to providers of electronic communications services. Since the conditions in Article 5(3) are clearly not satisfied for the deployment of spyware, it could be argued that the deployment constitutes a restriction of

[827] *Privacy International*, para 44 and *La Quadrature du Net and Others, para* 99.
[828] *Privacy International*, para 35 and *La Quadrature du Net and Others, para* 92.
[829] *Privacy International*, para 32.
[830] *La Quadrature du Net and Others*, para 103.

Obtenu pour vous par
Got for you by
agence europe

the right to protection of terminal equipment afforded by the ePD. This would put national laws on spyware within the scope of the ePD similar to national data retention laws. A recent preliminary question referred to the CJEU by an Austrian Court may give an answer to this question in the future.[831]

436. In comparison with the current ePD, the proposed eP Regulation would ensure that not all 'activities of the State in areas of criminal law' fall outside its scope, but only those law enforcement activities which fall within the corollary scope of the Law Enforcement Directive (LED) (Article 2(2)(d) e-privacy Regulation proposal).

Law Enforcement Directive

437. According to Article 2(3) of the LED, this directive does not apply to the processing of personal data in the course of an activity, which falls outside the scope of Union law. Article 13(3), 15 and 16(4) allow Member States to adopt legislative measures restricting or limiting the right of information, the right of access and the right to rectification of the data subjects among others in order to protect public security, national security and the rights and freedoms of others and to avoid prejudicing the prosecution of criminal offences.

438. Member States claiming a lawful use of Pegasus for LED purposes should at least prove its compliance with the LED, starting with pointing to a legal act clearly indicating the circumstances under which such tools may be used and how such use is necessary for the performance of specific tasks pursuant to Article 8 LED.

439. Besides the questionable uses of Pegasus for national security purposes, all uses for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, certainly fall under the scope of EU law.

440. The use of digital surveillance tools by EU Member State authorities for national security purposes, is also subject to national constitutional law as well as the relevant legal framework of the council of Europe, in particular the ECHR. In addition, the Convention 108 (recently modernised as Convention 108+) applies to processing of personal data for

[831] CJEU, C-548/21, *Bezirkshauptmannschaft Landeck*.

Obtenu pour vous par
Got for you by
agence europe

State (national) security purposes, including defence. The possible exceptions are subject to the conditions set by the Convention, and in any case, independent and effective review and supervision should be guaranteed.

c. European Convention of Human Rights (ECHR) and European Court of Human Rights (ECtHR)

441. The use of spyware interferes with the right to a fair trial, the right to respect for private and family life and with the right to freedom of expression and property enshrined respectively in Article 6[832], 8[833] and 10[834] ECHR and Article 1[835] of the Protocol to ECHR.

442. The ECtHR has repeatedly addressed the use of targeted communication surveillance and indiscriminate/bulk interception of communication data surveillance in law enforcement activities. In this respect, it has developed its own standard for assessing national legislation, which also includes a list of legal safeguards that should be applied to reduce the risk of abuse of power[836]. Any interference to these rights is only permitted if it is prescribed by law, pursues one of the legitimate aims set out in the Convention, is necessary in a democratic society and is proportionate to the legitimate aims pursued.

443. It also considers that the notion of national security should be clearly interpreted by domestic law and provide the scope of offences/crimes threatening the national security as well as other severe or exceptionally severe crimes allowing authorities to use secret surveillance measures to effectively prevent those crimes

444. State authorities are under an obligation to ensure effective mechanisms (including national courts, supervisory/monitoring mechanisms, public scrutiny) for avoiding arbitrariness and securing a fair balance between the right to privacy and the legitimate aim pursued by the interference. In order to assess the necessity and reasonableness of any intrusion in the private life or communication, any communication tapping or secret surveillance should be authorised by an independent and impartial domestic authority being vested with the relevant mandate and independent oversight should be ensured.

[832] https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf
[833] https://www.echr.coe.int/documents/guide_art_8_eng.pdf
[834] https://www.echr.coe.int/documents/guide_art_10_eng.pdf
[835] https://www.echr.coe.int/Documents/Guide_Art_1_Protocol_1_ENG.pdf
[836] See cases: *Big Brother Watch and Others v. the United Kingdom* [GC], no. 58170/13, 25 May 2021; Centrum för rättvisa v. Sweden, [GC], no. 35252/08, 25 May 2021

Obtenu pour vous par
Got for you by
agence europe

d. The Wassenaar Arrangement and Export control/dual use Regulation

445. The Wassenaar Arrangement[837] (WA) is a multilateral export control regime for controlling conventional arms and dual use goods and technologies. It was updated to include interception, intrusion and IP network surveillance technologies on its list of controlled items. The current participating states are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. However, because of Russia's non-constructive participation, the ability for consensus through this mechanism is increasingly limited.

446. WA defines intrusion software as "software specially designed or modified to avoid detection by monitoring tools, or to defeat protective countermeasures" and that either extracted data from a computer or network device or modified the "standard execution path" of a program to allow "the execution of externally provided instructions." This includes Spyware.

447. The aim of the WA is to prevent destabilising accumulations of conventional arms and dual-use goods and technologies — items with both civilian and military applications. However, the WA is not legally binding but Participating States regulate controlled items through their domestic export control regimes. Moreover, its transparency requirements appear inadequate. Some call for an overhaul of this arrangement and turn it into a binding treaty that takes account of human rights.[838] Several major arms exporters, including China, Israel, and Belarus, are not members of the WA, thereby opening a significant export controls loophole. Finally, while the WA limits the export of sensitive dual use goods and technologies to non- Participating States, it does not prohibit the purchase of surveillance technology from a non- Participating States. The import of Pegasus spyware to EU states demonstrates the weakness of this provision.

[837] https://www.wassenaar.org/
[838] https://rsf.org/en/pegasus-judicial-proceedings-france-offer-only-possibility-justice

Obtenu pour vous par
Got for you by
agence europe

448. On 9 September 2021 the Recast Dual Use Regulation EU No 2021/821[839] entered into force. The Regulation replaces EU No 428/2009 as the key legislative instrument, governing EU exports of so-called dual-use items.

449. The Recast Dual Use Regulation defines "cyber-surveillance items" as, "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems". The Regulation provides limited guidance on the new cyber-surveillance definition, noting only that the definition generally should not capture items for purely commercial applications such as billing, marketing, quality services, user satisfaction, or network security.

450. The Recast Dual Use Regulation provides for new rules on cyber-surveillance technology, the provision of technical assistance, as well as export restrictions for reasons of public security and human rights considerations. The Regulation does not include new Dual Use List entries for cyber-surveillance items. However, a new control category for cyber surveillance items has been created in connection to serious human rights violations. This new category is defined partly in non-technical terms – emphasising the capability for "surveillance", a concept strongly related to human right. [840] This applies to items (whether or not listed) that are specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems. The element of human rights assessment is integrated into the export licensing procedure for cyber surveillance items.

451. However, the Regulation does not provide criteria to determine what counts as a "serious" human rights violation or internal repression. Also, the recast version still leaves the opportunity for states to add their unique national licensing requirements, just like the WA, which could weaken the effectiveness of the export regime.

e. **The Budapest Convention on cybercrime of the Council of Europe**

[839] https://eur-lex.europa.eu/eli/reg/2021/821
[840] https://open.overheid.nl/repository/ronl-f616bafb-c268-436c-b926-3bacd98da61b/1/pdf/the-new-rules-for-export-control-of-cyber-surveillance-items-in-the-eu.pdf

Obtenu pour vous par
Got for you by
agence europe

452. The Budapest Convention is a criminal justice treaty that provides for (i) the criminalisation of a list of attacks against and by means of computers; (ii) procedural tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and (iii) international police and judicial cooperation on cybercrime and e-evidence. As of September 2022, 82 States are now either Parties (67), or have signed it or been invited to accede (15).

453. According to Article 1 of the Convention, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. Smartphones as we know them today should qualify as computer systems falling under the scope of the Convention.

454. In relation to spyware, Article 6(1)(a)(i) of the Convention states that: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5 […] with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5." The offences in Articles 2 through 5 are illegal access, illegal interception, data interference, and system interference, and the surveillance tools would serve for committing acts qualifying as illegal access and illegal interception.

455. According to the Explanatory Report to the Convention on Cybercrime, the provisions of the Convention which harmonise substantive criminal law do not apply to "conduct undertaken pursuant to lawful government authority".[841] Therefore, lawful State activities are not covered by the Convention, but it should be noted that interception of data according to Article 21 of the Convention is only allowed in relation to serious offences. The argument thus can be made that the Convention stipulates for the criminalisation of use of spyware by public authorities against persons not suspected for such offences.

f. Legal Professional Privilege and Professional Secrecy

[841] Explanatory Report to the Convention on Cybercrime, para 38: "The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences)."

Obtenu pour vous par
Got for you by
agence europe

456. Correspondence between a lawyer and his or her client, whatever its purpose, is protected under Article 8 of the ECHR, such protection being enhanced as far as confidentiality is concerned (Michaud v. France, §§ 117-119). This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants.

457. The ECtHR has emphasised that professional secrecy is the basis of the relationship of confidence existing between a lawyer and his client and any risk of impingement on it may have repercussions on the proper administration of justice. Without that trust, the client would not have the assurance that he can be full and frank with his lawyer, which is essential for providing full and accurate legal advice and support and is therefore a crucial guarantee for the fair trial process.

458. Directive 2013/48/EU foresees in Article 4 that "Member States shall respect the confidentiality of communication between suspects or accused persons and their lawyer in the exercise of the right of access to a lawyer provided for under this Directive. Such communication shall include meetings, correspondence, telephone conversations and other forms of communication permitted under national law".

459. The European Court of Justice states "*that confidentiality serves the requirements, the importance of which is recognized in all of the member states, that any person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it*", and adds that *the principle of "the protection against disclosure afforded to written communications between lawyer and client is based principally on a recognition of the very nature of the legal profession, inasmuch as it contributes towards the maintenance of the rule of law and that the rights of the defence must be respected*"[842].

460. The Court considered that the retention of traffic and location data for policing purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter and that such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistleblowers.

[842] ECJ, 1982, AM&S (155/79).

Obtenu pour vous par
Got for you by
agence europe

461. Moreover, the Court has not limited that consideration to matters relating to pending litigation only and has emphasised that, whether in the context of assistance for civil or criminal litigation or in the context of seeking general legal advice, individuals who consult a lawyer can reasonably expect their communication to be private and confidential (Altay v. Turkey).

462. In spite of its importance, the right to confidential communication with a lawyer is not absolute but may be subject to restrictions. In order to ensure that the restrictions that are imposed do not curtail the right in question to such an extent as to impair its very essence and deprive it of its effectiveness, the Court must satisfy itself that they are foreseeable for those concerned and pursue a legitimate aim or aims under paragraph 2 of Article 8, and are "necessary in a democratic society", in the sense that they are proportionate to the aims sought to be achieved.

463. It is necessary for the national law itself to state with sufficient clarity the scope of the discretion given to the competent or relevant authorities and the way in which this discretion is to be utilised, in order to provide an adequate safeguard against arbitrary interference.

464. The margin of appreciation of the State in the assessment of the permissible limits of interference with the privacy of consultation and communication with a lawyer is narrow in that only exceptional circumstances, such as to prevent the commission of serious crime or major breaches of prison safety and security, might justify the necessity of limitation of these rights.

465. Indirectly but necessarily dependent on the principle of professional secrecy is the right of everyone to a fair trial, including the right of anyone "charged with a criminal offence" not to incriminate themselves (Michaud v. France, § 118). While lawyer-client communications may concern matters which have little or nothing to do with litigation, there is no reason to distinguish between them, since they all concern matters of a private and confidential character; as a result, even though the conversation accidentally intercepted between the applicant and his client, did not consist, strictly speaking, of legal advice, the applicant was still entitled to the strengthened protection of lawyer-client communications

Obtenu pour vous par
Got for you by
agence europe

g. EU Procurement Laws

466. Member States' procurement contracts with respect to spyware and other surveillance systems are subject to the general rules and principles enshrined in the European Treaties as well as secondary Union law.

467. For decades, the defence sector has been considered as being outside the scope of application of EU law. From a legal standpoint, this is mainly due to the fact that Article 346(1)(b) of the Treaty on the Functioning of the European Union (TFEU) was read as excluding the whole defence sector from the remit of EU law[843]. The case law of the Court of Justice[844] seems to show that this is – instead – a case-by-case derogation that is to be applied strictly in exceptional situations and that the key conditions for the application of this Treaty provision are necessity and proportionality. Member States have to prove that the measures they take are necessary in order to protect their essential security interests, and that such an objective cannot be achieved through less restrictive means.[845]

468. Consequently, defence and security procurement contracts must abide by, inter alia, the principle of free movement of goods and the general principles of law set out by the Court of Justice, including transparency, necessity and proportionality.

469. Two Directives are relevant: Directive 2014/24/EU on public procurement[846] and Directive 2009/81/EC on Defence Procurement (contracts in the fields of defence and security)[847].

470. Directive 2014/24/EU applies in the context of law enforcement (including terrorism) as well as to mixed procurement[848] involving defence or security aspects (i.e. used for law enforcement and for national security purposes). Namely, where a single

[843] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12016E346
[844] See for instance Case C-615/10 https://curia.europa.eu/juris/document/document.jsf?docid=123604&doclang=EN
[845] https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_22_Article_346.pdf
[846] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0024
[847] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0081*
[848] Article 16: In the case of mixed contracts which have as their subject-matter procurement covered by this Directive as well as procurement covered by Article 346 TFEU or Directive 2009/81/EC, this Article shall apply.

Obtenu pour vous par
Got for you by
agence europe

contract is to be awarded, whether because its parts are not objectively separable or because objective grounds exist for awarding a single contract, where part of the contract is covered by Article 346 TFEU, the contract may be awarded without need to comply with EU law rules; or, if this is not the case and part of the contract falls within the scope of the Defence Procurement Directive, the contract may be awarded on the basis of the latter Directive.[849]

471. Article 15 of the Directive titled 'Defence and security', contains the basic provisions defining the law applicable to procurement having defence and security aspects. The default rule is that as soon as the public contract falls within the scope of the Defence Procurement Directive, the 2014 Directive will not apply, even if the public contract falls under one of the exclusions of the Defence Procurement Directive, which are listed in Articles 8, 12 and 13 of that Directive: if the contract falls under one of these exclusions, no EU public procurement directive will apply. Consequently, the default rule is that when a public contract or design contest in the fields of defence and security does not fall within the scope of the Defence Procurement Directive, then the 2014 Directive will apply

472. Directive 2009/81/EC on contracts in the fields of defence and security applies to contracts that are related to military or sensitive equipment, to other contracts for specific military purposes and to other sensitive contracts. Therefore, it should apply only to the extent to which the spyware is used for national security purposes. The Directive covers sensitive procurement for security purposes involving classified information and it aims to increase competition and transparency in defence markets between EU countries without compromising the security interests of Member States. The Directive aims to reduce Member States' use of Article 346 of the TFEU as it has placed the onus on Member States to justify why derogation is necessary given that the Directive explicitly takes into account the sensitive characteristics of defence procurement.

473. The Directive's broad ambit follows difficulties distinguishing between internal and external security matters and Member States' inconsistent definitions of "sensitive products". This issue has been exacerbated by the multiplicity of the defence-related product lists attached to the general licences.

[849] See European Public Procurement, Commentary on Directive 2014/24/EU, Elgar Commentaries series, Edited by Roberto Caranta and Albert Sanchez-Graells, Article 15 and Article 16 available at: https://www.elgaronline.com/view/edcoll/9781789900675/9781789900675.xml

Obtenu pour vous par
Got for you by
agence europe

474. While the Directive aims to increase intra-union competition, Member States and third countries party to the WTO plurilateral Agreement of Government Procurement 2012[850] (GPA) must likewise observe competition-enhancing principles in their dealings with each other, although contracts covered by the Directive (i.e. contracts relating to arms, munitions and war material awarded by contracting authorities/entities operating in the field of defence) are exempted from the application of the GPA.[851] Among other things, Parties must "maintain data that ensure the appropriate traceability of the conduct of covered procurement by electronic means" (Article XVI (3b) GPA).

475. However, Article III (1) GPA clarifies that, "Nothing in this Agreement shall be construed to prevent any Party from taking any action or not disclosing any information that it considers necessary for the protection of its essential security interests relating to […] procurement indispensable for national security…", allowing Parties to invoke Article III (1) in cases of sensitive procurements of products not specifically intended for military use.

h. **Safeguards in the EU Research Programmes**

476. Horizon 2020 was the EU's research and innovation funding programme from 2014-2020 with a budget of nearly €80 billion. Budget has been made available for research in a huge number of areas. The new funding programme until 2027 is the Horizon Europe programme with budget of €95.5 billions.

477. Regulation (EU) 2021/695 [852] establishes Horizon Europe. According to Article 19 "Actions carried out under the Programme shall comply with ethical principles and relevant Union, national and international law, including the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols." Furthermore, the Annotated Model Grant Agreement[853] describes the main ethical principles that should be respected. In relation to surveillance and spyware, the main

[850] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm
[851] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0081&from=EN, Recital 18
[852] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance).https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.170.01.0001.01.ENG&toc=OJ%3AL%3A2021%3A170%3ATOC
[853] Annotated Model Grant Agreement: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf

Obtenu pour vous par
Got for you by
agence europe

ethical principles are: Respecting human dignity and integrity; Ensuring privacy and confidentiality; Promoting justice and inclusiveness.

478. The European Commission published a guidance note on potential misuse of research on 7 January 2020[854]. In this regards, it considers that the research most vulnerable to misuse is, among others, research that involves developing surveillance technologies that could curtail human rights and civil liberties. It provides measures to take to address potential misuse of projects when planning research applications.

479. The claim has been made that Horizon 2020 and Horizon Europe funds have gone to technologies used in spyware. It is clear that funds have been made available to military and security companies, including Israeli defence companies Elbit and Israel Aerospace Industries. [855] [856]

480. The European Commission has stated that it has not found any evidence that would confirm the allegation that Horizon 2020 funds had been used to finance technologies developed by NSO Group.[857]

i. Spyware and Union development policies

481. The claim has been made that countries heavily dependent on foreign aid for their national budgets are high consumers of spyware technology, notably Rwanda.[858] The question is what fundamental rights and rule of law guarantees exist in Union development policies and to what extent development aid can be given if it is used for or enables acquisition of spyware by the receiving country.

482. The main legislative instrument within the development policies is Regulation (EU) 2021/947 - the 'Global Europe Regulation'.[859] According to Article 3(1)(a) one of the general objectives is to 'uphold and promote the Union's values, principles and fundamental interests worldwide'.

[854] Guidance note — Potential misuse of research: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf
[855] https://www.euractiv.com/section/innovation-industry/news/meps-denounce-eu-funding-of-israeli-defence-firms/
[856] https://euobserver.com/opinion/154902
[857] https://www.europarl.europa.eu/doceo/document/E-8-2018-006103-ASW_EN.html
[858] https://www.theguardian.com/commentisfree/2021/jul/23/rwanda-pegasus-surveillance
[859] https://eur-lex.europa.eu/eli/reg/2021/947/oj#ntc11-L_2021209EN.01000101-E0011

Obtenu pour vous par
Got for you by
agence europe

483. According to Article 8(1) in the Global Europe Regulation, the ‘Union shall seek to promote, develop and consolidate the principles of democracy, good governance, the rule of law, respect for human rights’. Article 8(2) further states that the Regulation shall be applied with ‘a rights-based approach encompassing all human rights, whether civil and political or economic, social and cultural in order to integrate human rights principles, to support the right holders in claiming their rights’.

484. Union funding may be provided through the types of financing envisaged by the Financial Regulation. As the respect for democracy, human rights and the rule of law is essential for sound financial management and effective Union funding as referred to in the Financial Regulation, assistance could be suspended in the event of degradation in democracy, human rights or the rule of law in third countries (Recital 40).

485. Persons and entities implementing financial instruments and budgetary guarantees shall comply with applicable Union law and principles and agreed international and Union standards as laid down in Article 155(2) and (3) of the Financial Regulation. The Commission shall assess whether the systems, rules and procedures of those persons and entities ensure protection of the financial interests of the Union equivalent to that provided for where the Commission implements the Union budget, with due regard to the principle of proportionality, taking into account the nature of the action and the conditions under which this action is implemented. Moreover, the Global Europe Regulation foresees, in Article 20, an incentive-based approach, stating that the progress of the partner countries shall be regularly assessed, in particular by means of progress reports, which include trends as compared to previous years.

486. It appears that more stringent control mechanisms should be implemented to ensure that financing from the Union development aid should not serve to fund or to facilitate the purchase of tools that could impinge on the principles of democracy, good governance, the rule of law and respect for human rights. Therefore, assessments of the compliance with the Financial Regulation made by the Commission should contain specific control criteria to avoid such abuses.

Obtenu pour vous par
Got for you by
agence europe

VI. Other Investigations and Judicial Proceedings

Polish Investigations on Pegasus

487. Despite their clear statutory obligations to investigate violations of law resulting from the acquisition and the use of Pegasus software, Polish prosecution services did not start ex officio any investigations. Ineffectiveness of prosecution services results from merging of functions of the Minister of Justice and the General Prosecutor.[860] The fact that the Minister of Justice continues to serve also as Prosecutor-General adds to the concerns over the independence of the Central Anti-Corruption Bureau from the executive power.[861] The increased supervisory powers of the Prosecutor-General, who can issue instructions in individual cases, including not to prosecute, and take over corruption cases of his subordinate prosecutors, provide avenues to influence anti-corruption prosecutions politically, which has also been the case on several occasions.[862]

488. Between June and July 2017, Mr Mikołaj Pietrzak (Dean of the Warsaw Bar), Ms Dominika Bychawska-Siniarska (a member of Helsinki Foundation for Human Rights), Ms Grabowska- Moroz (university lecturer), Mr Wojciech Klicki and Ms Katarzyna Szymielewicz (members of Panoptykon Foundation) filed on the basis of art 227 of the Code of Administrative Procedure complaints about certain provision of the national legislation governing secret surveillance. Due to not obtaining any legal remedy in Poland, the applicants are relying on art. 8 of the European Convention on Human Rights in their complaint that the secret systems for monitoring communications interfere with their right to respect for their private life, before the European Court of Human Rights. A hearing[863] took place in front of the ECHR on 27 September 2022[864]

489. Faced with the lack of fulfilment by Polish authorities of their statutory duties, victims of Pegasus attempt to trigger legal proceedings on their own initiative.

490. Prosecutor Ewa Wrzosek requested an initiation of criminal investigation of cyberattacks against her phone; in December 2021, District Public Prosecution Office in Warsaw refused to initiate criminal proceedings; at the end of September 2022, a court decision annulled the refusal by the District Public Prosecutor and ordered a detailed investigation.

---

[860] Prof. Dr Adam Bodnar, Opinia dla Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych Senatu RP, p. 7, Warszawa 2022, https://www.senat.gov.pl/gfx/senat/userfiles/_public/k10/komisje/2022/kni/15pos/15pos_ab.pdf

[861] As reported in the 2020 and 2021 Rule of Law Reports, Country Chapters on the rule of law situation in Poland, p. 8 and 11 (for 2020) and 18 (for 2021) ; GRECO Fifth Evaluation Round – Evaluation Report, paragraph 78.

[862] Helsinki Foundation (2022), A state of accusation: Polish prosecution service 2015-2022, and information received from the Batory Foundation in the context of the country visit to Poland and as reported, with more details, in the 2020 Rule of Law Report, Country Chapter on the rule of law situation in Poland, pp. 8 and 11. In this context, see also the concerns raised by the Venice Commission (opinion CDL-AD(2017)028).

[863] https://www.echr.coe.int/Pages/home.aspx?p=hearings&w=7203817_27092022&language=en&c=&py=2022 Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland (application nos. 72038/17 and 25237/18).

[864] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef

Obtenu pour vous par
Got for you by
agence europe

491. Senator Krzysztof Brejza requested an initiation of criminal investigation concerning illegal invigilation of his mobile phone by Central Anti-corruption Office, as well as a manipulation of his SMS messages and making such manipulated SMS messages available to media. After lengthy review by a number of prosecution offices, the District Public Prosecution Office in Ostrow Wielkopolski initiated an investigation concerning an acquisition of access to data on Senator's phone.[865] Faced with inactivity of public prosecution services, Senator Krzysztof Brejza initiated numerous legal actions concerning the defamation campaign that was directed against him on the basis of manipulated SMS messages. In January 2022 his civil law action against Jaroslaw Kaczynski for slander, related to Pegasus, was at first dismissed by Bydgoszcz District Court. In October 2022, the district court's decision has been declared null and void by the Gdansk Appellate Court and sent for a new adjudication.

Polish Senate Inquiry Committee

492. On January 12th, 2022, Senate constituted a Special Committee to inquire on cases of illegal surveillance, their impact on election process in Poland and reform of special services[866]. It held and continues to hold numerous meetings both with victims and experts.

493. The Senate extraordinary committee does not have investigative powers, which allows those invited to appear before the committee to decline without facing consequences. On the contrary, the lower house (Sejm), which is in the hand of the ruling party, has investigative powers and could open a committee of enquiry but is unlikely to do so due to the majority in that house.

494. The Senate extraordinary committee was set up in January 2022 and has so far held 16 meetings and questioned 33 witnesses and experts[867], Testimonies of victims that testified during hearings organised by the Senate's Special Committee, univocally indicate that the use of Pegasus in Poland was motivated politically and that there were no grounds of national security that could be invoked for the use of the spyware.

495. The Senate's Special Committee established that:

a. "the purchase of the Pegasus system, the use of the system, is a violation of the Polish order, it is a violation of the Constitution, [...].

- "the possibility of using such an operational control device, and above all just such a leaky device, capable of manipulating the obtained data, as is the case with Pegasus, [...] introduces an absolute inequality of candidates running in the elections"[868]

[865] https://www.gov.pl/web/po-ostrow-wielkopolski/wszczecie-postepowania-z-zawiadomienia-krzysztofa-brejzy
[866] https://www.senat.gov.pl/prace/komisje-senackie/komisja,215,komisja-nadzwyczajna-do-spraw-wyjasnienia-przypadkow-nielegalnej-inwigilacji-ich-wplywu-na-proces-wyborczy-w-rzeczypospolitej-polskiej-oraz-reformy-sluzb-specjalnych.html
[867] https://www.senat.gov.pl/prace/komisje-senackie/posiedzenia,215,2,komisja-nadzwyczajna-do-spraw-wyjasnienia-przypadkow-nielegalnej-inwigilacji-ich-wplywu-na-proces-wyborczy-w-rzeczypospolitej-polskiej-oraz-reformy-sluzb-specjalnych.html
[868] Transcript of the testimony of Prof. Dr Andrzej Zoll.

Obtenu pour vous par
Got for you by
agence europe

b. the expert before the Senate's Special Committee also affirmed that "when it comes to the 2019 elections [...] if we were at the time when the process of affirmation, validation or invalidity would take place in the Supreme Court, the establishment of such a practice [as the use of Pegasus] would obviously lead to the annulment of the election".[869]

-in the light of current binding Polish provisions regarding application of judicial and operational control, the use of Pegasus is not admissible, cannot be accredited nor certified,[870] and constitutes a crime under art. 231, art. 267, art. 269b(1) and art. 130(2) of the Polish Penal Code.[871]

496. Wrongdoing Ministers and officials (e.g. Mariusz Kaminski[872], Maciej Wąsik, Andrzej Stróżny[873], Ernest Bejda[874]) refused to appear before the Senate's Special Committee, obstructing its inquiry proceedings in violation of the Act on the performance of the mandate of a deputy and senator of May 9, 1996, according to which representatives of competent state bodies are obliged to present information and explanations at the request of permanent and extraordinary senate committees on matters falling within their scope of activity; as well as in a violation of art. 112, in connection with art. 124 of the Constitution, according to which the manner of performing the constitutional and statutory duties of state organs towards the Senate is specified in the Regulations of the Senate; and in a violation of art. 60(3) of the Senate's rules of procedure obliging representatives of state bodies to cooperate with the committee, in particular to actively participate in committee meetings. They also refused to appear in front of the European Parliament inquiry Committee.

Complaints and Lawsuits in Greece

497. The victims of surveillance, but also others, have brought various lawsuits and complaints to the prosecutors and the courts, reported in the media, as follows:

498. On 24 February 2022, news site Solomon filed a legal complaint against EYP before the prosecutor of the Supreme Court for the spying on their journalists, including Mr Stavros Malichudis.[875]

499. On 3 May 2022, media reported that a preliminary investigation had already been launched by the head of the Athens Prosecutor's Office, Sotiria Papageorgopoulou, to

[869] Idem.
[870] Prof. Dr hab. Dariusz Jagiełło, Opinia prawna dotycząca oceny legalności używania do realizacji czynności operacyjno-rozpoznawczych systemu „Pegasus", Kancelaria Senatu, Warszawa 2022, https://www.senat.gov.pl/gfx/senat/userfiles/_public/k10/dokumenty/bad/2022/oe-425.pdf
[871] Prof. Dr hab. Mariusz Bidziński, Ocena legalności i skutków prawnych działań podejmowanych przy użyciu systemu Pegasus, Kancelaria Senatu, Warszawa 2022, https://www.senat.gov.pl/gfx/senat/userfiles/_public/k10/dokumenty/bad/2022/oe-426.pdf
[872] https://www.senat.gov.pl/gfx/senat/userfiles/_public/k10/komisje/2022/knwpni/inne/pismo_ministra_sprawwewn.pdf
[873] https://www.senat.gov.pl/gfx/senat/userfiles/_public/k10/komisje/2022/knwpni/inne/odpowiedz_szefa_cba_a._strozneg o.pdf
[874] https://www.senat.gov.pl/gfx/senat/userfiles/_public/k10/komisje/2022/knwpni/inne/odpowiedz_b._szefa_cba_e._bejdy .pdf
[875] https://wearesolomon.com/mag/accountability/solomon-files-complaint-against-intelligence-agency/

Obtenu pour vous par
Got for you by
agence europe

determine if there has been a criminal violation of communications privacy of Mr Thanasis Koukakis.[876]

500. On 26 July 2022, Mr Nikos Androulakis filed a criminal complaint at the Prosecutor's Office of the Supreme Court for attempting to infect and monitor his cell phone through Predator.[877]

501. On 27 July 2022, Mr Koukakis appealed to the European Court of Human Rights against Greece.

502. On 5 August 2022, media reported that Supreme Court prosecutor Isidoros Dogiakos had launched a criminal investigation into the leaks of classified information to journalists who broke the story.[878]

503. Mr Grigoris Dimitriadis has brought five legal defamation claims (Strategic Lawsuits Against Public Participation - SLAPPs) against newspaper Efimerida ton Syntakton (EFSYN), investigative online portal Reporters United and their reporters Mr Nikola Leontopoulos and Mr Thodoris Chondrogiannos, and freelance journalist Mr Thanasis Koukakis. The lawsuits range from between €150,000 and €250,000. On 20 October Mr Dimitriadis was awarded the 'SLAPP Politician of the Year Award' 2022 by the Case Coalition[879] at its European Anti-SLAPP contest 2022.[880][5]

504. On 9 September 2022, Christos Spirtzis, former minister and Syriza MP, was informed that his phone had been hacked by Predator and reported it to the chief prosecutor.[881]

505. On 5 October 2022,[882] Koukakis filed a lawsuit with prosecutors in Athens accusing Intellexa and its personnel (Mr Dilian and another shareholder – Sara Hamou, who is also Dilian's ex-partner) of criminal offenses, including breaches of privacy and communications laws by allegedly selling their Predator spyware to EYP, supporting that it is illegal in respect of European and Greek law.[883]

506. On 6 November 2022, the Greece's Supreme Court ordered a probe following the report including over 30 politicians, journalists and businessmen that were targeted by state surveillance.[884]

---

[876] https://govwatch.gr/en/sovares-apokalypseis-kai-diethneis-antidraseis-gia-tin-parakoloythisi-dimosiografoy-apo-tin-eyp-kai-to-logismiko-ypoklopon-predator/
[877] https://www.reuters.com/world/europe/greek-socialist-leader-files-complaint-over-attempted-phone-bugging-2022-07-26/
[878] https://balkaninsight.com/2022/08/23/how-many-greek-spyware-scandal-just-getting-started-says-targeted-reporter/
[879] https://www.the-case.eu/
[880] https://www.article19.org/resources/greece-slapp-drop-lawsuits/
[5] https://www.article19.org/resources/greece-slapp-drop-lawsuits/
[881] https://www.euractiv.com/section/digital/news/another-greek-opposition-lawmaker-victim-of-predator/
[882] https://www.news247.gr/koinonia/skandalo-ypoklopon-minysi-kata-tis-intellexa-apo-ton-thanasi-koykaki.9781771.html
[883] https://www.haaretz.com/israel-news/security-aviation/2022-10-07/ty-article/.premium/criminal-allegations-against-israeli-linked-spyware-ex-intel-commander-in-hacking-scandal/00000183-ad14-d3f8-a9ef-bf5752e60000
[884] https://www.euractiv.com/section/justice-home-affairs/news/top-greek-court-orders-probe-into-wiretap-scandal-report/

Obtenu pour vous par
Got for you by
agence europe

Greek Parliamentary Committee on Institutions and Transparency and temporary Parliamentary Committee of Inquiry

507. The Special Permanent Committee on Institutions and Transparency is one of the four special committees in the Hellenic Parliament and is permanent.[885] It is in charge of exerting parliamentary control and oversight over the EYP and its actions. The Committee on Institutions and Transparency held several hearings. On 29 July 2022, it interrogated the directors of ADAE and EYP. The head of the EYP, Panagiotis Kontoleon, stated at this hearing that the EYP did indeed carry out surveillance of Koukakis for national security reasons, but that he had no knowledge of the attempt to hack Androulakis' phone with Predator.[886]

508. On 30 August, the Committee called nine people in for a closed-door hearing, including the recently resigned former head of EYP Panagiotis Kontoleon, public prosecutor Vasiliki Vlachou and former Secretary General Grigoris Dimitriadis. All three evaded answering questions by invoking confidentiality.[887] Former EYP commanders Giannis Roubatis and Theodoros Davillas were also heard, as well as the Prosecutor of the Court of Appeals Konstantinos Tzavelas, and the president of the ADAE Christos Rammos (1 September 2022).

509. The Committee of Inquiry (29 August to 10 October 2022), which had very wide statutory powers combining parliamentary control with the investigative powers of the prosecutor, was established on the basis of a Pasok proposal during the Greek parliamentary plenary session of 29 August 2022.[888] Its mandate of one month was to examine the violation of the confidentiality of the communications of Nikos Androulakis by the National Intelligence Service (EYP) or by other natural or legal persons, the confirmed attempt to trap his mobile phone with the Predator malware, its illegal use in the territory and the investigation into the existence of responsibilities of the Prime Minister Mr. Kyriakos Mitsotakis and any other natural person involved or a legal person, as well as the of the case of EYP infection with Predator of the mobile of Athanasios Koukakis and the case of the call center of the KKE.

510. The President, Vice-President, and Secretary of the Committee were all from the New Democracy party, as were the majority of its members. The parliamentary political parties all submitted their final reports on the Committee's investigations on 10 October 2022.[889]

511. New Democracy concluded that the government had properly responded, that the parliament had properly investigated the issue, and that "there was no evidence to suggest that the Prime Minister, his office and his associates were aware of the lifting of secrecy at

[885] https://en.wikipedia.org/wiki/Special_Permanent_Committee_on_Institutions_and_Transparency
[886] https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)733637
[887] https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi
[888] https://www.reuters.com/world/europe/greek-parliament-sets-up-inquiry-commission-probe-phone-tapping-scandal-2022-08-29/
[889] https://www.politico.eu/article/greek-spyware-inquiry-ends-in-stalemate/

Obtenu pour vous par
Got for you by
agence europe

any stage." Their final report relies on the NTA audit to show that the EYP did not use Predator and highlights the need to strengthen the institutional guarantees for the operation of the EYP by re-introducing the requirement of involving a second prosecutor to lift confidentiality. At the political level, the government also assumed the strict political responsibility of the Androulakis case, with the resignations of the Secretary General of the Prime Minister and the EYP commander. [890]

512. The parties SYRIZA[891], PASOK-KINAL and The Communist Party of Greece[892] (KKE) adopted minority reports criticising the conclusion of the majority's report and stated that there was sufficient evidence that EYP used the illegal predator software, and asked for further investigations by both the Greek parliament and the criminal justice system. It also noted that the choice of witnesses to call in for testimony was in the hands of the party majority and that the bureau of the Committee rejected witnesses proposed by the opposition parties.

Complaint and Investigation in Cyprus

513. On 25 June 2020, Makarios Drousiotis, Cypriot investigative journalist and former presidential advisor said that, after finding significant evidence of surveillance and hacking into his writing, personal messages and home security system, he would file a new complaint to Cypriot authorities and share it with the EU Commission.[893]

Complaints in Hungary

514. The Hungarian Civil Liberties Union (HCLU) announced on 27 January 2022[894] that it was launching several complaints on behalf of six of its clients before the Hungarian authorities[895], and was also launching foreign procedures[896], including with the European Commission, the European Court of Human Rights in Strasbourg and a complaint in Israel.

515. On behalf of journalists Brigitta Csikász, Dávid Dercsényi, Dániel Németh and Szabolcs Panyi, as well as student activist Adrien Beauduin and a sixth person who requested anonymity, the organisation pursued the legal remedies offered by the National Security Act. It has lodged complaints with the ministers overseeing the secret services and initiated an investigation by the National Security Committee of Parliament and the Commissioner for Fundamental Rights. Besides these, the HCLU has lodged so-called subject access requests with the secret services to gain information on possible data processing and would take legal action before the courts and the National Authority for Data Protection and Freedom of Information, depending on the answers.

[890] https://www.ieidiseis.gr/politiki/167157/nd-gia-eksetastiki-katerrefsan-oi-kataggelies-tis-antipolitefsis
[891] https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi
[892] https://www.ieidiseis.gr/politiki/167119/ypoklopes-oi-porismatikes-theseis-tou-kke-gia-tin-eksetastiki-epitropi
[893] https://www.occrp.org/en/daily/12631-cypriot-journalist-says-he-is-being-spied-on-and-fears-for-his-life
[894] https://hclu.hu/en/articles/pegasus-case-hclu-takes-coordinated-domestic-and-foreign-legal-action
[895] https://hclu.hu/en/pegasus-case-hungarian-procedures
[896] https://hclu.hu/en/pegasus-case-foreign-procedures

Obtenu pour vous par
Got for you by
agence europe

516. On behalf of the student activist, they lodged a complaint with the Commission and asked it to investigate whether his rights to freedom of residence and employment guaranteed by the Treaty on the Functioning of the European Union had been violated (university education is also considered to be a form of employment according to the interpretation of the Court of Justice of the European Union).

517. The HCLU also launched a multitude of lawsuits before the European Court of Human Rights on behalf of journalists and members of Civil Society organisations stigmatised by the government, as they are ostensibly highly exposed to surveillance.

518. Finally, HCLU also filed a complaint with the Israeli Attorney General on behalf of three of their clients. They asked him to investigate whether a criminal offence had been committed when the NSO Group obtained a state export licence for Pegasus knowing that such a spy weapon could be more easily misused by the government in Hungary than in other countries.

519. On 22 July 2021[897], one week after the revelations of the consortium lead by Forbidden Stories, Hungarian prosecutors opened a probe into suspected unlawful surveillance following multiple complaints of misuse of the Israeli-made Pegasus spyware. The Budapest Regional Investigation Prosecutor's Office said in a statement that the investigation would examine "the so-called Pegasus case, under the suspicion of the crime of gathering unauthorised secret information". However, on 15 June 2022, the Hungarian investigative prosecutors terminated the investigation into allegations of illegal eavesdropping on the mobile phones of several Hungarian journalists and opposition figures in connection with Pegasus spyware, citing "absence of a crime".[898] Referring to certain people named in the press who were allegedly spied on, the public investigators said people on whom the authorities secretly collected information for law enforcement or national security purposes were not necessarily criminal suspects, and in such cases they examined whether these people had been caused harm in anyway. The findings were negative, the investigators said.

Investigations in Spain

520. In April 2022 the Spanish government announced it would investigate reports of spying on Catalan and Basque pro-independence leaders.[899] In parallel Félix Bolaños[900], Minister of the Presidency, Relations with the Cortes and Democratic Memory announced an internal inquiry to check whether Spain's Intelligence Agency had access to Pegasus. The investigations come after a study by Citizen Lab, published by the New Yorker, that revealed that dozens of pro-independence Catalan politicians, journalists, and activists were targeted with the spyware between 2015 and 2020.

[897] https://hungarytoday.hu/hungary-pegasus-investigation-prosecution-public-prosecutor-office/
[898] https://dailynewshungary.com/hungarian-prosecutors-drops-probe-into-pegasus-spyware/
[899] https://www.euronews.com/2022/04/25/spain-begins-investigation-into-catalonia-pegasus-spyware-allegations
[900] https://www.euronews.com/2022/04/25/spain-begins-investigation-into-catalonia-pegasus-spyware-allegations

Obtenu pour vous par
Got for you by
agence europe

521. Spain's High Court[901] opened its own investigation after the government said Pegasus software was used to spy on ministers, including Prime Minister Sanchez[902]. As part of a so-called investigative commission to investigate the spying, the Court called the chief executive officer of Israel's spyware software Pegasus firm NSO Group and Parliamentary Affairs Minister Felix Bolanos to testify as witnesses. The investigative judge also interviewed former Director of the National Intelligence Centre Paz Esteban, who was removed from office in the wake of the significant security breach resulting from the surveillance scandal,[903] [904]as well as the Defence and Interior Ministers, whose devices were among those hacked. The Court[905] sent a formal request for international judicial assistance, to the Israeli government asking for information on "different aspects of the software tool". The High Court has also lifted the secrecy of the documents related to the case and overturned a ban on investigating wiretapping of mobile phones belonging to Prime Minister Pedro Sánchez and Defence Minister Margarita Robles.

522. In June 2022, Morocco filed a lawsuit against a Spanish journalist for his reporting on the Moroccan government and intelligence services using Pegasus against him and others. [906]

"CatalanGate" Complaints in other Member States

523. Legal action is underway in a number of other EU Member States, including France, Belgium, Switzerland, Germany, and Luxembourg, as a result of the surveillance carried out on the Catalan separatists who are in exile.[907]

Investigation by Prosecutor's Office in Bulgaria

524. On 11 February 2022, the Prosecutor's Office of Sofia announced that it started an investigation to inquire if the Pegasus Spyware has been illegally used by Bulgarian government entities to spy on Bulgarian citizens. It has requested information from the Bulgarian special services and the National Bureau for Control of Special Intelligence Means as to whether state entities have used the spyware.

525. It will also investigate whether Pegasus software was sold in Bulgaria, and to which actors. At the time of writing, the investigation was still ongoing, so no conclusions have been published yet.[908]

[901] https://www.reuters.com/world/spanish-court-calls-ceo-israels-nso-group-testify-case-spying-with-pegasus-2022-06-07/
[902] https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware
[903] https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html
[904] https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations
[905] https://www.thelocal.es/20220607/spanish-judge-seeks-to-quiz-israeli-ceo-over-spyware-scandal/
[906] https://www.middleeastmonitor.com/20220705-morocco-files-lawsuit-against-spain-journalist-who-reported-use-of-pegasus-spyware/
[907] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab , *19 April 2022.*
[908] https://bnr.bg/en/post/101599684/sofia-city-prosecutor-s-office-investigates-possible-use-of-pegasus-spyware-in-bulgaria

Obtenu pour vous par
Got for you by
agence europe

German Investigations and FinFisher

526. On 5 July 2019, the Society for Civil Rights (GFF), Reporters Without Borders Germany (RSF Germany) the blog netzpolitik.org and the European Center for Constitutional and Human Rights (ECCHR) filed criminal complaints against several high ranking CEOs[909] of the Munich-based companies for exporting the spyware FinSpy to Turkey without an export license. It appears that FinFisher may have got around the export ban by operating a parallel business structure. Following the complaint, on 5 September 2019, the Munich public prosecutor's office initiated preliminary proceedings on suspicion of violation of the Foreign Trade and Payments Act, which can result in a fine of up to five years imprisonment.

527. On October 2020, the public prosecutor's office and the German Customs Investigation Bureau (ZKA) searched[910] a total of 15 properties (business premises and private apartments) around Munich and a company from the group of companies in Romania

528. On 28 March 2022, the Public Prosecutor's Office Munich seized the company's accounts, after which FinFisher GmbH and its two partner companies declared insolvency in February 2022.

529. Moreover, on 22 September 2021, the Society for Civil Rights (*Gesellschaft für Freiheitsrechte*) lodged a complaint with the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) on the use of Pegasus by the German intelligence service (BKA) [911]. The complaint raises issues of unlawful outsourcing of sovereign powers, insufficient safeguards against unauthorised access and deletion, unlawful commissioning of data processing, insufficient functional limitations, unlawful modifications of the target system, and the illegal exploitation of security vulnerabilities.

Microsoft vs DSIRF and Investigation in Austria

530. On July 27 2022, Microsoft's Threat Intelligence Center (MSTIC) and the Microsoft Security Response Center (MSRC) released in a technical blog post[912] that they caught an Austrian company selling spyware based on previously unknown Windows exploits. The new details were published to coincide with written testimony given by the software

[909] https://legacy.freiheitsrechte.org/home/wp-content/uploads/2019/11/2019-07-04-FinFisher-Strafanzeige-EN.pdf. The list includes: Mr Markus Meiler and Mr Holger Rumscheidt, CEOs of Elaman GmbH; Mr Carlos Gandini, CEO of FinFisher GmbH; Mr Lucian Hanga and Mr Holger Tesche, CEOs of Finfisher Labs GmbH, as well as additional staff members whose names are unknown of Elaman GmbH, Finfisher GmbH, and Finfisher Labs GmbH.
[910] https://www.business-humanrights.org/en/latest-news/german-spyware-company-finfisher-searched-by-public-prosecutors/
[911] https://freiheitsrechte.org/en/presse/pressemitteilungen/pm-pegasus
[912] https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

Obtenu pour vous par
Got for you by
agence europe

company to a House Intelligence Committee hearing on commercial spyware and cyber surveillance.

531. Microsoft linked a number of cyberattacks to a threat group it calls "Knotweed," better known as the Vienna-based intelligence-gathering company, Decision Supporting Information Research Forensic, or DSIRF. The group targets entities in Europe and Central America with a surveillance tool dubbed Subzero. On its website, DSIRF says it was founded in 2016 but claims to have over two decades of experience delivering "data-driven intelligence to multinational corporations in the technology, retail, energy and financial sectors," as well as offering red team testing, where hackers are given permission to find and exploit security vulnerabilities during product testing.[913]

532. Microsoft said in its report that Knotweed has been active since at least 2020 and developed spyware — dubbed Subzero — that allows its customers to remotely and silently break into a victim's computer, phone, network infrastructure and internet-connected devices.[914] Subzero is similar to NSO Group's Pegasus and Candiru's DevilsTongue spyware in functionality and is often used by governments to monitor journalists, activists and human rights defenders. It is understood that the spyware from DSIRF was targeting law firms, banks and consultancies in at least three countries[915]. Microsoft confirmed that the exploit used by DSIRF has now been patched in a security update[916].

533. On 2 August[917], Austria announced it was investigating the report that links DSIRF to spyware targeting entities in at least three countries. A statement published by Austria's interior ministry[918] reads that "DSN (the National Security and Intelligence Directorate) checks the allegations. So far, there is no proof of the use of spy software from the company mentioned". The investigation is ongoing.

Investigations in France

534. On 22 June 2021[919], four executives of Amesys and Nexa Technologies were indicted by investigating judges of the Paris Judicial Court for complicity in torture in the Libyan portion of the investigation and complicity in torture and enforced disappearance in the Egyptian portion. Both companies[920] are prosecuted for providing surveillance

[913] https://techcrunch.com/2022/07/28/dsrif-spyware-windows-zero-day/ _
[914] https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/
[915] https://www.infosecurity-magazine.com/news/austria-spyware-law-firms-finance/
[916] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22047
[917] https://securityaffairs.co/wordpress/133911/malware/austria-investigates-dsirf-firm.html
[918] https://www.securityweek.com/austria-probes-claim-spyware-targeted-law-firms-banks
[919] https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/france-judicial-investigation-opened-regarding-nexa-technologies-surveillance-equipment-sale-to-egyptian-regime/
[920] https://www.lemonde.fr/pixels/article/2022/09/29/les-logiciels-espions-sont-des-outils-tres-dangereux-devastateurs-guilhem-giraud-un-ancien-du-renseignement-se-confie_6143630_4408996.html

Obtenu pour vous par
Got for you by
agence europe

technology to authoritarian regimes in Libya and Egypt.[921] The judicial investigation has also been extended to include the sale of surveillance technology to Saudi Arabia.

535. Moreover, on 20 July 2021[922], the Paris prosecutor's office opened an investigation into spying on French journalists and on one of Emmanuel Macron's cell phones by Morocco, following criminal complaints launched by Reporters Without Borders (RSF). On 1 July 2022[923], the Paris Public Prosecutor's Office entrusted an investigating judge from his cyber section with the investigation. The investigation will cover many potential offences, including criminal association, state agents acting as an organised gang in the accessing and maintaining of an automated data processing system, intercepting correspondence sent by electronic means, installing devices liable to allow such interception, and possessing and disseminating words or images infringing privacy.

536. Morocco, accused of having used the Pegasus spyware through his intelligence agency, decided to sue Amnesty and Forbidden Stories for defamation before the Paris Criminal Court on 22 July 2022. And on 29 July 2022[924], four new direct citations in defamation were made against the daily Le Monde and its director Jérôme Fenoglio, a third is suing Mediapart and its boss Edwy Plenel, and the last attacks Radio France. A first procedural hearing was scheduled for October 15 before the chamber specializing in press law, but if a trial is held, it should not take place for about two years.

Israeli Inquiry

537. Israeli economic newspaper Calcalist published a series of articles beginning on 18 January 2022, accusing the Israeli National Police (INP) of using the Pegasus spyware to infiltrate the telephones of Israeli citizens, including government ministries, social activists, and corporate executives, without court approval.[925]

538. In response to the allegations, Israel's attorney general at the time, Avichai Mandelbilt, appointed an Internal inspection team at the Ministry of Justiceon 31 January 2022, to investigate the veracity of the claims presented in the Calcalist articles. The inquiry was furthermore tasked with determining whether or not the use of spyware is compatible with current Israeli law regulating police wiretapping and search powers, notably the 1979 Wiretapping Law[926] and the 1969 Arrest and Search Ordinance[927]. The INP was ordered to suspend its use of spyware until the inquiry's conclusion.

[921] https://www.ldh-france.org/surveillance-et-torture-en-egypte-et-en-libye-des-dirigeants-damesys-et-nexa-technologies-mis-en-examen/ and https://www.france24.com/fr/france/20210622-cybersurveillance-en-libye-et-en-%C3%A9gypte-4-chefs-d-entreprises-fran%C3%A7aises-mis-en-examen

[922] https://www.france24.com/fr/france/20210720-affaire-pegasus-le-parquet-de-paris-ouvre-une-enqu%C3%AAte-sur-l-espionnage-de-journalistes

[923] https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/projet-pegasus-l-enquete-francaise-sur-le-logiciel-espion-confiee-a-un-juge-d-instruction_5233438.html

[924] https://fom.coe.int/en/alerte/detail/104525764

[925] https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html

[926] https://www.nevo.co.il/law_html/law01/077_001.htm

[927] https://www.nevo.co.il/law_html/law01/055_128.htm

Obtenu pour vous par
Got for you by
agence europe

539. The team was comprised of Amit Merari, Deputy Attorney General for Criminal Matters, Eyal Dagan, the former ISA Chief of Investigations, and Tsafrir Kats, the former Head of the ISA Technology Section.[928]

540. Since it was an internal investigation team at the Ministry of Justice, there was public and media criticism in Israel of its independence and the integrity of its work, and on conflicts of interest. In any case, this team did not have investigative powers enshrined in the 1969 Law on Investigative Committees[929] (proposals in the Knesset and by government ministers to establish an official committee were not promoted for political reasons) .

541. In the course of the investigation, the team examined a database provided by NSO Group containing information on phones infected by Pegasus. According to a statement from the Ministry of Justice, around 1500 phone numbers were checked.[930]

542. The inquiry team published an interim report on 21 February and a final report on 1 August, 2022, largely exonerating the INP[931]. The former stated that they had found no indications that the Israeli police targeted Israeli citizens without a judicial warrant.

543. The final report generally confirmed this position, and it was found that all recorded uses of spyware were in fact directed at legitimate targets for whom the police authorities had acquired court approval. However, although wiretapping warrants had been acquired, the inquiry team discovered four cases in which the authorities had targeted persons in excess of the terms of the warrants.[932]

544. Furthermore, the report did establish that there was a need for structural changes concerning the use of spyware by the INP. They use a version of Pegasus called Saifan alongside a few other spyware programs, which collects collateral information irrelevant to criminal investigations. As a result, the report recommends that Saifan's capacity to collect legally impermissible material be blocked through technological manipulation in order to reduce the risk of exploitation. It also recommends the development of a new, more comprehensive format for reporting spyware usage. At a more general level, the inquiry team expressed concern about the INP's introduction of Saifan and other spyware programs without having consulted with the police department's legal advisers and the office of the attorney general. The report's most far-reaching recommendation is the call for new digital surveillance legislation—but the effect of such a call is offset by the legal conclusion that existing law authorises the (cautious) use of spyware.

545. One of the arguments of conflict of interest was that it was an internal committee of the Ministry of Justice, which was also supposed to examine the propriety of the supervision

[928] https://www.lawfareblog.com/stay-calm-and-proceed-caution-merari-report-israeli-polices-pegasus-scandal
[929] https://www.nevo.co.il/law_html/law00/71810.htm
[930] https://www.reuters.com/world/middle-east/israeli-inquiry-checking-nso-database-over-police-wiretap-allegations-2022-02-13/
[931] https://www.haaretz.com/israel-news/2022-02-21/ty-article/.premium/investigators-release-findings-showing-no-pegasus-misuse-by-israel-police/0000017f-efc1-df98-a5ff-efedaa0f0000
[932] https://www.lawfareblog.com/stay-calm-and-proceed-caution-merari-report-israeli-polices-pegasus-scandal

Obtenu pour vous par
Got for you by
agence europe

carried out by the Ministry of Justice on the use of the Pegasus system. For example, one of the committee's conclusions was that the Ministry of Justice was not aware of the capabilities of the Pegasus system. This conclusion caused eyebrows to be raised: the power of the Pegasus system had already caused an international uproar for years due to the exposure of its use in other countries, and there were even discussions in Israeli courts about its export, in which the Ministry of Defence was represented by lawyers from the Ministry of Justice.[933]

546. Finally, it must be noted that, although some parts of the Calcalist story were proven wrong by the Merari report, some prominent experts in Israeli privacy law have maintained that given the dramatic impact of such technology on the right to privacy, the police cannot justify the utilisation of spyware on the basis of existing legislation developed with much less intrusive technology in mind.[934]

Investigations in the United States

547. The New York Times reported in January that the US Federal Bureau of Investigation (FBI) had procured the Pegasus spyware in 2019 under the Trump administration. The Times investigation showed that testing of Pegasus began in June 2019 in an FBI facility in New Jersey. It was also reported that the FBI received demonstrations of Phantom by the NSO, a spyware capable of infiltrating US telephone numbers.[935]

548. Christopher A. Wray, the Director of the FBI, participated in a congressional hearing initiated by the House Intelligence Committee in March and revealed that the FBI had purchased a "limited license" for testing and evaluation purposes and to better understand what security concerns arise in conjunction with its use.[936] In an emailed response to inquiries from The Guardian concerning the FBI's procurement of Pegasus, the need to "stay abreast of emerging technologies and tradecraft" was furthermore cited as a motivation to test the spyware.[937]

549. Despite this claim of intended use, a 2018 letter from the FBI to Israel's Ministry of Defence informed the Israeli government that the US government had purchased Pegasus with the intention of collecting data from mobile phones in order to aid ongoing criminal investigations. The letter was reviewed by the New York Times. There is, therefore, a possibility that the FBI considered using Pegasus in an operational capacity. According to the New York Times investigation, the US Department of Justice and the FBI reached an agreement not to deploy spyware purchased from the NSO Group in an operational capacity only last summer (2021). [938]

[933] Eitay Mack, Israeli lawyer and expert on NSO
[934] https://www.calcalist.co.il/local_news/article/hj2eihlt9
[935] https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
[936] https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Transcript-20220308.pdf
[937] https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware
[938] https://www.nytimes.com/2022/05/12/us/politics/fbi-pegasus-spyware-israel.html

Obtenu pour vous par
Got for you by
agence europe

550. Nevertheless, an unidentified source cited by the New York Times stated regarding the FBI's use of Pegasus, "They weren't using it at all. Like, not even switching it on. But they kept paying for it, and they wanted to renew. It was a one-year test project and it cost about $5m [£3.7m], and they renewed for another $4m, but they didn't use it."[939]

551. In 2017, the FBI was already investigating the role of Israeli spyware vendor NSO Group Technologies in possible hacks on American residents and companies as well as suspected intelligence gathering on governments[940]. The probe was underway by 2017, when Federal Bureau of Investigation officials were trying to learn whether NSO obtained from American hackers any of the code it needed to infect smartphones, said one person interviewed by the FBI then.

552. Moreover, in 2021, the US Department of Justice (DOJ), was reportedly showing renewed interest in NSO[941]. DOJ lawyers approached the messaging app WhatsApp with technical questions about the alleged targeting of 1,400 of its users by NSO Group's government clients in 2019. And in February 2022, following revelations by a whistleblower of a tentative by NSO to gain access to global cellular networks, which help cellular companies route calls and services, it was announced that further investigations were carried by the DOJ [942].

553. The US Congress has pursued various actions to address the matter of the use of spyware to date. In addition to the March hearing featuring Christopher A. Wray, the US House Intelligence Committee held a hearing on Commercial Cyber Surveillance on July 27, 2022, to discuss Pegasus' impact on national security policy.[943]

554. The latest version of the Intelligence Authorisation Act for Fiscal Year 2023 was introduced in the Senate on 12 July, 2022[944], and includes provisions meant to further regulate the spyware industry in the United States.[945] The bill would, inter alia, "provide authority for the Director of National Intelligence (DNI) to bar any contract with these foreign firms by the IC".[946] It also authorises (but does not require) the DNI to block intelligence community contracts with U.S. companies that acquire, in whole or in part, any foreign spyware tool and it grants the President new authority to sanction foreign spyware companies, their executives, and foreign government officials who target American officials with spyware.[947] The National Defence Authorisation Act for Fiscal Year

[939] https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware
[940] https://www.reuters.com/article/us-usa-cyber-nso-exclusive/exclusive-fbi-probes-use-of-israeli-firms-spyware-in-personal-and-government-hacks-sources-idUSKBN1ZT38B
[941] https://www.theguardian.com/world/2021/mar/01/israeli-spyware-firm-nso-group-faces-renewed-us-scrutiny
[942] https://www.washingtonpost.com/technology/2022/02/01/nso-pegasus-bags-of-cash-fbi/
[943] https://intelligence.house.gov/videos/#:~:text=On%20Wednesday%2C%20July%2027%2C%202022,hearing%20on%20commercial%20cyber%20surveillance.
[944] https://www.congress.gov/bill/117th-congress/senate-bill/4503/text
[945] https://intelligence.house.gov/uploadedfiles/iaa_ans_xml.pdf
[946] https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=1209
[947] https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=1211

Obtenu pour vous par
Got for you by
agence europe

2022 passed last December furthermore required the State Department to compile an annual list of spyware vendors with which to avoid business ties.[948]

Blacklisting by US Department of Commerce

555. On November 3, 2021, the Commerce Department's Bureau of Industry and Security (BIS) has released a final rule[949] adding four foreign companies to the Entity List[950] pursuant to paragraph 744.11(b) of the Export Administration Regulations (EAR) for engaging in activities that are contrary to the national security or foreign policy interests of the United States. NSO Group and Candiru (Israel), were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order. The two other companies added are Positive Technologies (Russia), and Computer Security Initiative Consultancy PTE. LTD. (Singapore). They were added to the Entity List based on a determination that they traffic in cyber tools used to gain unauthorised access to information systems, threatening the privacy and security of individuals and organisations worldwide.

556. The Entity List is a tool utilized by BIS to restrict the export, reexport, and in-country transfer of items subject to the EAR to persons (individuals, organisations, companies) reasonably believed to be involved, have been involved, or pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States. For the entities, BIS imposes a license requirement that applies to all items subject to the EAR. In addition, no license exceptions are available for exports, reexports, or transfers (in-country) to the entities being added to the Entity List in this rule. BIS imposes a license review policy of a presumption of denial for these entities.

Council of Europe Inquiry

557. The Council of Europe's Parliamentary Assembly appointed Dutch MP Pieter Omtzigt[951] as rapporteur for the Committee on Legal Affairs and Human Rights on "Pegasus and similar spyware and secret state surveillance". He published the first results of his work after 3 months, in April 2022[952].

[948] https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=1209
[949] https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list
[950] https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file last checked on 25 October 2022
[951] https://www.rtlnieuws.nl/tech/artikel/5303665/pieter-omtzigt-nso-group-pegasus-spyware-spionagesoftware-onderzoek-rapporteur
[952] A draft memorandum is available at https://storage.googleapis.com/pieter-omtzigt-website/documenten/Pegasus-memorandum-Omtzigt.pdf.

Obtenu pour vous par
Got for you by
agence europe

558. The CoE also released a report in June 2022 on the impact of Pegasus spyware on human rights[953]. The report provides a technical description of the Pegasus spyware and analyses the impact it may have on human rights and fundamental freedoms, in particular the right to privacy and freedom of expression. The report places a special emphasis on the legal instruments and standards that the CoE has at its disposal to uphold fundamental rights and ensure stronger protections against mass or targeted unlawful and unjustified surveillance.

559. In the report, the CoE mentioned the minimum requirements developed by the Court[954], which should be set out in domestic law to avoid abuses of power when it comes to targeted communication tapping: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; the circumstances in which intercepted data may or must be erased or destroyed.

560. The Modernised Convention 108+ (Convention) broached in the report requires improved data quality, increased protection for sensitive data, high level data security, greater fairness, transparency and accountability from public authorities and private companies, including developers and service providers, who should proactively demonstrate compliance with the data protection rules.

561. Not to contravene Article 8 of the ECHR, systems of secret surveillance should contain adequate and effective safeguards against abuse, including independent supervision[955].

META vs NSO and Apple vs NSO

562. META (Facebook, WhatsApp) sued the Israeli hacker-for-hire company NSO Group on 29 October 2019[956] in U.S. federal court for allegedly targeting some 1,400 users of its encrypted messaging service WhatsApp with highly sophisticated spyware.[957] The lawsuit filed in San Francisco is the first legal action of its kind, according to Facebook, involving a nearly totally unregulated realm. META claimed that NSO Group violated laws including the U.S. Computer Fraud and Abuse Act with a crafty exploit that took advantage of a flaw in the popular communications program allowing a smartphone to be penetrated through missed calls alone.

[953] https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8
[954] See cases of Huvig v. France, no 11105/84, 24 April 1990; Kruslin v. France, no 11801/85 24 April 1990; Valenzuela Contreras v. Spain, no. 27671/95, 30 July 1998, Weber and Saravia v. Germany no. 54934/00, 29 June 2006.
[955] Recommendation CM/Rec(2016) 4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors - https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415d9#_ftn1
[956] https://www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup/whatsapp-sues-israels-nso-for-allegedly-helping-spies-hack-phones-around-the-world-idUSKBN1X82BE
[957] https://www.courtlistener.com/docket/16395340/facebook-inc-v-nso-group-technologies-limited/

Obtenu pour vous par
Got for you by
agence europe

563. NSO has requested that the court dismiss the lawsuit on the basis of sovereign immunity, claiming that they should be viewed as an agent for the foreign governments that are their clients. The NSO request was denied finally in June 2022 after NSO lost an appeal to the US Supreme Court regarding whether they could defend themselves on the basis of sovereign immunity.[958] As NSO has lost its motion for dismissal, the court proceedings continue. The further calendar is not known.

564. Apple filed a lawsuit against NSO on 23 November 2021 to hold it accountable for the surveillance and targeting of Apple users. To prevent further abuse and harm to its users, Apple is also seeking a permanent injunction to ban NSO Group from using any Apple software, services, or devices. Apple's legal complaint provides new information on NSO Group's FORCEDENTRY, an exploit for a now-patched vulnerability previously used to break into a victim's Apple device and install the latest version of NSO Group's spyware product, Pegasus. The exploit was originally identified by the Citizen Lab, a research group at the University of Toronto. The spyware was used to attack a small number of Apple users worldwide with dangerous malware and spyware.[959]

565. In its lawsuit Apple states that NSO are "notorious hackers—amoral 21st century mercenaries who have created highly sophisticated cyber-surveillance machinery that invites routine and flagrant abuse. They design, develop, sell, deliver, deploy, operate, and maintain offensive and destructive malware and spyware products and services that have been used to target, attack, and harm Apple users, Apple products, and Apple. For their own commercial gain, they enable their customers to abuse those products and services to target individuals including government officials, journalists, businesspeople, activists, academics, and even U.S. citizens". [960]

566. NSO has requested that the court dismiss the lawsuit on the basis of (a) sovereign immunity, (b) forum non-convenience, (c) failure to join an indispensable party, and (d) failure to state a claim.[961] Apple has contested the motion to dismiss. The court has not yet pronounced itself on the motion. The above-mentioned decision by the US Supreme Court in the case META vs NSO, would mean that the NSO claim for sovereign immunity would fail also in this case.

567. With respect to the claim that the Apple lawsuit should be dismissed on basis of the argument that Apple has failed to join indispensable parties, i.e. the national governments that are NSO's clients, NS has stated that they do not know which devices are hacked, not have any access to the data downloaded. It should however be noted that when NSO appeared in the PEGA Committee, it was stated that the Pegasus backend installed on a proprietary server of the client from with the client hacks phones and downloads data, contained a locked part which NSO access in case of complaints to check that the client has

[958] https://globalfreedomofexpression.columbia.edu/cases/whatsapp-inc-v-nso-group-technologies-limited/
[959] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf
[960] https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf
[961] https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/28/

Obtenu pour vous par
Got for you by
agence europe

used Pegasus in conformity with the agreed terms and with respect to human rights. It should also be noted that each model of phone and operative system requires a specific version of the Pegasus spyware, which means that separate versions of the spyware is developed for Apple's products.

568. The further timeline of the Apple vs NSO proceedings is not known.

Obtenu pour vous par
Got for you by
agence europe

V. The European Union's capacity to respond

569. 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.[962] This is not because there are legal constraints, but rather because it is a political choice. The 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

570. 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.

571. 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.

572. 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

[962] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

Obtenu pour vous par
Got for you by
agence europe

Commission implementation report[963] 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

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

European Council and Council

574. 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.[964] 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.

575. 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.

576. 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

[963] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223
[964] Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

Obtenu pour vous par
Got for you by
agence europe

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

577. 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.

578. 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.

579. 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[965], 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.

580. On 28 September 2022, PEGA wrote a letter to Europol[966], urging it to make use of its new powers under Article 6 of the Europol Regulation.[967] In a letter of reply dated 13 October 2022[968], 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

[965] 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
[966] https://twitter.com/EP_PegaInquiry/status/1576855144574377984
[967] "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."
[968] File no 1260379

Obtenu pour vous par
Got for you by
agence europe

Member State concerns the abuse of spyware by EU Member State governments or by third countries.

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

582. Paradoxally, 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."[969]

European judiciary

583. 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.[970] 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

584. 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 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.

[969] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ
[970] Appeal by Koukakis to the European Court of Human Rights, 27 July 2022

Obtenu pour vous par
Got for you by
agence europe

VI. Areas for action

585. The work of the PEGA inquiry committee has highlighted the urgent need for action at EU level in a number of areas. Issues that merit policy initiatives are set out in this chapter.

Moratorium

586. It is clear that the trade in, and use of spyware needs to be regulated strictly. However, it is likely that such regulation will take considerable time. Therefore, a moratorium on the sale, acquisition, transfer, and use of spyware should be adopted immediately. The moratorium may be lifted on a country-by-country basis, only if the following conditions have been fully met:

a. All cases of alleged abuse of spyware are fully investigated and resolved without delay by the appropriate law enforcement, prosecutorial and judicial authorities; and
b. Proof that the framework governing the use of spyware is in line with the standards laid down by the Venice Commission and relevant case law by the ECJ and ECtHR[971] [972]; and
c. The explicit commitment to accede to a request by Europol pursuant to Art 6(1a) of the Europol Regulation relating to investigations into allegations of illegitimate use of spyware[973]; and
d. Repeal of all export licenses that are not fully in line with both the letter and the spirit of the Dual Use Regulation.

587. The European Commission shall assess whether the fulfilment of these criteria for lifting the moratorium have been met.

Common standards and a legal framework for the use of spyware

588. Currently the national frameworks for the use of spyware are widely divergent, and in many cases wholly inadequate. There is a clear need for common EU standards regulating the use of spyware by government bodies. The Venice Commission has already laid down useful criteria for the use of surveillance by law enforcement and intelligence agencies[974]

[971] Venice Commission, Report on the democratic oversight of the security services, 15 December 2015, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e
Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf
[972] Venice Commission, Opinion on the Act Of 15 January 2016 Amending The Police Act And Certain Other Acts, 13 June 2016, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e
[973] 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
[974] Venice Commission, Opinion on the Act Of 15 January 2016 Amending The Police Act And Certain Other Acts, 13 June 2016, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e

Obtenu pour vous par
Got for you by
agence europe

and for democratic oversight of security services.[975] Additionally, there is ample relevant case law from the CJEU[976] and the ECtHR as well as recommendations by civil society.[977] EU standards shall cover at least the following elements:

a. A closed list of authorities allowed to use spyware;
b. A limited and closed list of crimes for which the use of spyware is allowed;
c. Transparency: when a Member State has purchased spyware, it must be auditable to an independent, impartial audit body. Member States should publish, as a minimum, the number of requests for surveillance approved and rejected, and the type and purpose of the investigation. Member States should anonymously register each investigation in a national register with a unique identifier so that it can be investigated in case of suspicions of abuse.
d. The requirement of meaningful *ex-ante* judicial authorisation by an impartial and independent judicial authority, which demonstrates the necessity and proportionality of the envisaged measure and includes all available information. Given that spyware allows for retroactive access to messages, files and metadata, specific rules must be drawn up for this kind of surveillance;
e. The right of notification for the targeted citizen: after the surveillance has ended, the authorities should notify the citizen of the fact that they were subject to the use of spyware by the authorities. Information regarding the date and duration of the surveillance, the warrant issued for the surveillance operation, data obtained, information on how that data has been used and by which actors and the date of deletion of the data should also be provided. The notification should be done without undue delay, unless an independent judicial authority grants delay of notification, in case immediate notification would seriously jeopardise the purpose of the surveillance.
f. Effective and independent *ex-post* oversight: there must be effective and independent oversight over the use of spyware by public agencies. Such independent oversight bodies shall have all required means and powers to exercise meaningful oversight. Parliamentary oversight bodies shall have cross-party membership and full access to information.
g. Effective, meaningful legal remedy for direct and indirect targets: individuals who claim to be adversely affected by surveillance should have access to redress through an independent body. Legal remedies must be effective in both law and fact. Remedies must be known and accessible. They require swift, thorough and impartial investigation by an independent oversight body. They must also be capable of ending on-going violations and failings by having access, expertise and technical capabilities to handle all relevant data and to actually be able to determine whether the security assessment made by the authorities of an individual is reliable and proportionate. When violations are of such a grave nature, criminal prosecution should be required;

[975] Venice Commission, Report on the democratic oversight of the security services, 15 december 2015, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e
[976] Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, para 175
Judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238
Judgment of 15 February 2016, *N.*, C601/15 PPU, EU:C:2016:84, para 50
Judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, para 156
[977] Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf

Obtenu pour vous par
Got for you by
agence europe

h. Provisions on the deletion of data: during surveillance, authorities should delete all irrelevant data. After the surveillance and the investigation for which the authorisation was granted has ended, authorities should delete the data as well as any related documents, such as notes that were taken during that period. The deletion must be recorded, and the records should be auditable;
i. Limits to the duration of the operation: the act of hacking and spying should only last as long as is strictly necessary. The judicial authorisation beforehand should be for a specified duration, and the hacking can only be extended when further judicial authorisation is granted for another specified duration. Given the nature of spyware and the possibility of retroactive surveillance, the judicial authorisation should define the precise scope of the operation;
j. The obligation to use a version of spyware that is programmed in such a way that it minimises the access to data: the spyware should not have access to all data stored on a device, but should be programmed in such a way that it limits access to data to the minimum of what is strictly necessary.
k. A non-exhaustive but binding list of privileged professions, such as lawyers, journalists, politicians, and doctors that shall not be targeted by spyware;
l. The obligation for Member States to notify each other in case of surveillance of citizens or residents of another Member State.

Definition of "national security"

589. Member State authorities have referred to "national security" as justification for the use of spyware and for absolute secrecy and lack of accountability. As the Commission has pointed out[978][979], a mere reference to national security by national authorities is not sufficient to exclude the application of EU law, so national security cannot be interpreted as being an unlimited carve out from the normal rules. Member States must be able to demonstrate that national security is compromised when it uses spyware.

590. Not all Member States may have a clear definition of "national security", and there can be big differences between the national regimes. A common European definition of "national security" is needed which lays down criteria to determine what legal regime applies in matters of national security, as well as a clear demarcation of the area where such a special regime may apply.

Better enforcement of existing legislation

591. Although new regulation is needed, much can be achieved by properly enforcing existing legislation. Not only does a lack of enforcement of EU law prevent any protection of EU citizens' fundamental rights against the use of spyware, it also harms the efforts of the

[978] Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022
[979] Response letter by Commissioners Hahn and Reynders to the rapporteur - 14 October 2022

Obtenu pour vous par
Got for you by
agence europe

EU to come across as a serious interlocutor on fundamental rights on a global level. The following EU laws have been identified as relevant but not properly enforced:

a. Anti Money Laundering Directive (in particular provisions on the Ultimate Beneficial Owner)
b. e-Privacy, General Data Protection Regulation, Law Enforcement Directive
c. Procurement rules
d. Dual Use Regulation
e. Case law (rulings on surveillance and national security)
f. EU Whistleblower Directive

592. The European Commission has to investigate and report on the shortcomings in implementation and enforcement, and put forward a detailed and ambitious road map for fixing the shortcomings by summer 2023 at the latest.

593. In addition to new legislation, the European Parliament shall take the initiative to launch an inter-institutional conference. During this conference, the Parliament, Commission and Council must aim for governance reforms that strengthen the EU institutional capacity to respond adequately to attacks on democracy and rule of law from the inside. The EU needs effective supranational methods for enforcing EU law and Treaties in the case of non-compliance by Member States.

Export rules

a. Wassenaar Arrangement

594. The Wassenaar Arrangement as multilateral export control regime for conventional arms and dual use goods and technologies should be modified as follows:

595. The mandate of the Wassenaar Arrangement is currently focused on the promotion of transparency and prevention of destabilising accumulations of dual use goods and technologies. Human rights considerations are however not included within the remit of its mandate. Therefore, the arrangement ought to include a human rights framework that embeds the licensing of spyware technologies. In addition, such a framework would equally assess and review the compliance of companies producing these technologies.[980]

596. The Wassenaar Arrangement limits the export of sensitive dual use goods and technologies to non-participating states, but does not prohibit the purchase of surveillance technologies from non-participating states. The Wassenaar Arrangement should therefore include the prohibition of the purchase of surveillance technologies from states that are not part of the Wassenaar Arrangement.

[980] Amensty International. Operating from the Shadows. Inside NSO Group's corporate structure.

Obtenu pour vous par
Got for you by
agence europe

597. Cyprus is one of the export hubs of the EU and approximately 29 Israeli spyware companies are now registered in Cyprus.[981] It is therefore of utmost importance that Cyprus becomes a signatory of the Wassenaar Arrangement, as the last EU Member State to do so. All efforts must be made by the EU to enable Cyprus to join.

598. The Wassenaar Arrangement is not binding for the participating states. It is thus highly dependent on the voluntary contributions of national governments. Different domestic export control regimes can cause a race to the bottom, incentivising the move of spyware companies to countries were the arrangement's objectives are not properly enforced. As a first step, the Wassenaar Arrangement should therefore become binding on all its signatories. In the long run, the Wassenaar Arrangement should work towards an international treaty.

b. Dual Use Legislation

599. In the light of the spyware revelations, the European Commission shall conduct an in-depth investigation of export licences granted for the use of spyware under the EU Dual Use Regulation.

600. The revised EU Dual Use Regulation entered into force only recently, in 2021. Nevertheless, it is clear that the Commission's evaluation of the implementation by the Member States must go beyond the mere assessment of the legal transposition of EU laws. The Commission assessment must ensure that the rules are effectively applied on the ground. Measures must be taken to close loopholes, such as cutting up a spyware product into separate entities so as to escape the requirement of a license under the EU Dual Use Regulation.

601. Stronger enforcement of the EU Dual Use regulation:

a. The European Commission has to immediately launch an in-depth investigation into the application of the EU Dual Use Regulation in practice, taking into account all relevant sources;

b. The European Commission needs to regularly check and properly enforce the EU Dual Use Regulation to avoid 'license shopping' throughout the EU, as is currently the case in Bulgaria and Cyprus. The Commission should have adequate resources for this task.

c. Stronger provisions that should be included in a future recast of the Regulation:

d. For the sake of transparency and accountability, the EU Dual-Use regulation should ensure detailed reports are provided from the designated national authorities responsible for the approval and denial of export licenses for dual use items. Such a report should be made public on a quarterly basis and include:

   i. The dual use item in question;
   ii. The amount of licenses applied for;
   iii. The name of the export country;
   iv. A description of the export company and whether this company is a subsidiary;
   v. A description of the end user and destination;

[981] Makarios Drousiotis. State Mafia. Chapter 6. Published 2022.

Obtenu pour vous par
Got for you by
agence europe

vi. The value of the export license;
vii. Why the export license was approved or denied

e. At this moment, for the purpose of monitoring and evaluation by the Commission, Member States can actually withhold information in light of commercials sensitivity, defence and foreign policy or national security reasons. In a future recast, all this information should be provided to the Commission. However, in order to prevent sensitive information becoming available to third countries, the Commission can decide to classify certain information in its annual report. A dedicated standing parliamentary committee should be set up, with access to such classified information, for the purpose of parliamentary oversight.

f. The recast of the Dual-Use Regulation defines cyber-surveillance items as: '[...] dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems.' This definition should be broadened to include the following technologies as well: mobile telecommunications interception or jamming equipment; intrusion software; IP network communications surveillance systems or equipment; software specially designed or modified for monitoring or analysis by law enforcement; laser acoustic detection equipment; forensic tools which extract raw data from a computing or communications device and circumvent "authentication" or authorisation controls of the device; electronic systems or equipment, designed either for surveillance and monitoring of the electro-magnetic spectrum for military intelligence or security purpose; and Unmanned Aerial Vehicles capable of conducting surveillance.[982]

g. The recast of the EU Dual-Use regulation stipulates that *"An authorisation shall be required for the export of cyber-surveillance items not listed in Annex I if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law."*[983] However, the regulation does not define what is considered a serious violation of human rights. The regulation should therefore include a more robust interpretation of human rights protection and violation, as outlined by the EU Charter of Fundamental Rights, the Court of Justice of the EU, and the European Court of Human Rights.[984]

h. A dedicated European Export Control Agency should be set up to oversee the export of dual use products by the Member States.

602. Additional European legislation should require corporate actors producing and/or exporting surveillance technologies to include human rights and due diligence frameworks in line with the UN Guiding Principles on Business and Human Rights (UNGPs).[985]

[982] Reporters without borders. NGO coalition including RSF reacts to EU's new dual use export rules.
[983] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), Art 5(1)
[984] Amnesty International. New EU Dual Use Regulation agreement 'a missed opportunity' to stop exports of surveillance tools to repressive regimes.
[985] Reporters without borders. NGO coalition including RSF reacts to EU's new dual use export rules.

Obtenu pour vous par
Got for you by
agence europe

Due diligence

603. All companies involved in trade in spyware within or from the EU, have to be subject to due diligence standards, including vetting procedures of their clientele, and report to the Commission on an annual basis on compliance.

Relations with third countries

604. The European Union shall start talks with the US administration about a joint strategy and joint standards, including a joint white list and black list of spyware vendors that are or are not authorised to sell their products to public authorities. These joint standards should address common criteria for vendors to be included in either list, arrangements for common US-EU reporting on the industry, common scrutiny and due diligence obligations for vendors. Both the EU and US should make the sale of spyware to non-state actors a criminal offence.

605. The EU-US Trade and Technology Council shall hold wide and open consultations with civil society for the development of these joint strategy and standards.

Relations with third countries

606. The European Union must also start talks with other countries, in particular Israel, with a view to establishing a common framework for the issuance of marketing and export licenses for surveillance technologies. Such a framework shall also include rules on transparency about the list of eligible countries and the due diligence arrangements.

Zero-day vulnerabilities

607. Without prejudice to the NIS2 Directive and the upcoming Cyber Resilience Act, the discovery, sharing, patching and exploitation of vulnerabilities should be regulated, including, but not limited to, the following elements:

a. The right for information researchers to research vulnerabilities, and share their results. The civil and criminal liability provisions should therefore be adapted in the Cybercrime Directive and Copyright Directive.
   Large organisations should demonstrate that they create incentives for information researchers to actively participate in vulnerability research, by investing in *i.a.* proper vulnerability treatment plans, good disclosure practices within the industry and with civil society, and run bug bounty programmes in order to prevent security researchers from selling zero-day vulnerabilities to (potentially) malicious actors.
b. A ban on the commercial trade in vulnerabilities, and an obligation to disclose the findings of vulnerability research to the organisations that can patch them. Each organisation should therefore have a publicly available contact point where vulnerabilities can be disclosed in a standardised way. Organisations that receive information about vulnerabilities in their system need to act immediately to fix the exploit.

Obtenu pour vous par
Got for you by
agence europe

c. State authorities should not purchase, keep open, or stockpile any vulnerabilities. The longer vulnerabilities are stockpiled, the greater the chance that they will be discovered and exploited by other parties before they can be fixed by the software vendor. Vulnerabilities should be patched as quickly as possible in a vulnerability management system, and should be made public afterwards.
d. However, only in specified cases, state authorities can keep vulnerabilities for a limited time to exploit them. Each Member State should therefore have a vulnerability equity process, set in law, with necessity/proportionality test for the decision to disclose or withhold each vulnerability, and strict rules on delaying notification. This should be subject to strict oversight by an independent supervising body.

Telecom networks

If telecom providers are able to recognise and block ransomware on their network, they should also be able to identify and block spyware that will break into the user's device.
The global messaging system known as SS7 should be better secured to avoid simple breaches in communication on mass and individual level.
If any state actor has an access point to the SS7 network, the license of the main operator through which the state actor has access, should be revoked.
The currently unlimited possibility for unknown individuals to buy any number for any country in the world available should be regulated, so malicious activity will be more difficult to hide.
Telecom providers should take action against spoofing.

ePrivacy Regulation

608. The ePrivacy Regulation should be adopted as soon as possible and should fully reflect the case law on the restrictions for national security as well as the need to prevent abuse of surveillance technologies. The new ePrivacy Regulation should strengthen the fundamental right to privacy and its scope for surveillance should not go beyond the ePrivacy Directive.

Europol

609. All indications of illegitimate spyware use must be investigated. In exceptional cases, when the national authorities are unable or unwilling to investigate, and in particular when there is a justified concern that evidence may be destroyed, Europol must be allowed to investigate and secure evidence. To this end, Europol should use its newly acquired powers under Regulation (EU) 2022/991 and to propose to competent authorities of the Member States concerned to initiate, conduct or coordinate a criminal investigation.[986] The Member States should commit to honouring the proposals of Europol.

[986] 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

Obtenu pour vous par
Got for you by
agence europe

610. In addition, the Europol Regulation should be adapted, so that in exceptional cases Europol can also start a criminal investigation without the approval of the Member State.

611. A register shall be set up within Europol of law enforcement operations involving the use of spyware. Each operation should be identified with a code.

612. Spyware abuse by governments must be included in the annual Internet Organised Crime Threat Assessment (IOCTA) report by Europol.

EU Development aid

613. More stringent control mechanisms should be implemented to ensure that financing from the Union development aid does not serve to fund or facilitate the purchase of tools that could impinge on the principles of democracy, good governance, the rule of law and respect for human rights. Therefore, assessments of the compliance with the Financial Regulation made by the Commission should contain specific control criteria to avoid such abuses.

Financial institutions

614. Respect for human rights by the financial sector must be enhanced. To this end, the UNGPs 10+ recommendations must be transposed into EU law, and the Due Diligence Directive must fully applied to the financial sector.[987]

Implementation of previous resolutions of European Parliament

615. Many recommendations of the *European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* are still valid after eight years. They should therefore be carried out as a matter of urgency;

616. (74.) Stresses that, despite the fact that oversight of intelligence services' activities should be based on both democratic legitimacy (strong legal framework, ex ante authorisation and ex post verification) and adequate technical capability and expertise, the majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;

617. (75.) Calls, as it did in the case of Echelon, on all national parliaments which have not yet done so to install meaningful oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate; calls on the national parliaments to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal

[987] https://www.ohchr.org/en/special-procedures/wg-business/financial-sector-and-human-rights

Obtenu pour vous par
Got for you by
agence europe

means, including the right to conduct on-site visits, to be able to effectively control intelligence services;

618. (76.) Calls for the setting up of a High-Level Group to propose, in a transparent manner and in collaboration with parliaments, recommendations and further steps to be taken for enhanced democratic oversight, including parliamentary oversight, of intelligence services and increased oversight collaboration in the EU, in particular as regards its cross-border dimension;

619. (77.) Considers this High-Level group should:

a. define minimum European standards or guidelines on the *ex-ante* and *ex-post* oversight of the intelligence services on the basis of existing best practices and recommendations by international bodies, such as the UN and the Council of Europe, including the issue of oversight bodies being considered as a third party under the 'third party rule', or the principle of 'originator control', on the oversight and accountability of intelligence from foreign countries;

b. set strict limits on the duration and scope of any surveillance ordered unless its continuation is duly justified by the authorising/oversight authority; recalls that the duration of any surveillance ordered should be proportionate and limited to its specific purpose;

c. develop criteria on enhanced transparency, built on the general principle of access to information and the so-called 'Tshwane Principles'[988];

620. (78.) Intends to organise a conference with national oversight bodies, whether parliamentary or independent;

621. (79.) Calls on the Member States to draw on best practices so as to improve access by their oversight bodies to information on intelligence activities (including classified information and information from other services) and establish the power to conduct on-site visits, a robust set of powers of interrogation, adequate resources and technical expertise, strict independence vis-à-vis their respective governments, and a reporting obligation to their respective parliaments;

622. (80.) Calls on the Member States to develop co-operation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);

623. (81.) Calls on the Commission to present, a proposal for an EU security clearance procedure for all EU office holders, as the current system, which relies on the security clearance undertaken by the Member State of citizenship, provides for different requirements and lengths of procedures within national systems, thus leading to differing treatment of Members of Parliament and their staff depending on their nationality;

624. (83.) Recalls the provisions of the inter-institutional agreement between the European Parliament and the Council concerning the forwarding to and handling by Parliament of classified information held by the Council on matters other than those in the

[988] The Global Principles on National Security and the Right to Information, June 2013.

Obtenu pour vous par
Got for you by
agence europe

area of the common foreign and security policy, which should be used to improve oversight at EU level;

Research

625. While the work of Citizen Lab at Toronto University has been key in revealing the large scale of targeting and infections with spyware via forensic analysis, the EU should not be dependent on a third country institute for this important work. The Commission should therefore initiate the creation of an independent European interdisciplinary institute, with a focus on research and development at the nexus of information and communication technology, fundamental rights, and security, which will also discover and expose the unlawful use of software for illicit surveillance purposes.

Rule of Law

626. The impact of the illegitimate use of spyware is much more pronounced in Member States where authorities that would normally be tasked with investigating and providing redress to victims, are captured by the State. In other words, where a Rule of Law crisis exists, the national authorities cannot be relied upon. This is why the Commission should step in pro-actively with its Rule of Law toolbox, particularly to do the following:

627. Put in place a more comprehensive monitoring of the Rule of Law, including assessing the responsiveness of State institutions to provide redress to victims of spyware, in particular to journalists. This also links to long-standing demands of Parliament for the Commission to broaden the scope of its annual Rule of Law report and include all challenges to Democracy, the Rule of Law and Fundamental Rights as included in Article 2 TEU;

628. Pro-actively pursue and bundle infringement procedures against Member States for Rule of Law deficiencies, such as threats to the independence of the judiciary and the effective functioning of the police and prosecutorial services. This is crucial for the victims of spyware to be able to get access to remedies and redress;

629. Broaden the Commission assessment for the purpose of the Rule of Law budget conditionality regime, in particular looking at the impacts of the use of spyware on the accountability of public spending. As journalists and politicians are hampered in their work to ensure accountability over the spending of EU funds, the use of spyware could be a factor in the assessment of the Commission of whether there are Rule of Law breaches which threaten the EU financial interests.

Obtenu pour vous par
Got for you by
agence europe

EU Ligitation Fund

630. An EU Litigation Fund should be set up without undue delay, fully in line with the Preparatory Action adopted by the European Parliament in 2017, to create an "EU fund for financial support for litigating cases relating to violations of democracy, rule of law and fundamental rights"[989], which the Commission has only partially implemented so far. A litigation fund should cover the actual litigation costs and enable the victims of spyware to seek adequate redress.

European Commission, Council and European Council

631. The European Commission shall make full use of all its powers as guardian of the Treaties, to conduct a comprehensive and in-depth investigation into the abuse of and trade in spyware in the EU;

632. The Commission must conduct a full-blown inquiry into all allegations and suspicions of the use of spyware against EU Commission officials, and report to the European Parliament as well as to the responsible law enforcement authorities;

633. Literally, on the eve of the publication of this draft report, the PEGA committee received a reply from the Council to the queries of the European Parliament, which were sent to all individual Member States. Considering that members of the Council and European Council are directly implicated, and given the magnitude of the treat to democracy in Europe, the European Council has to dedicate a summit meeting to the matter and conduct its own inquiry.

European Parliament

634. The European Parliament should have full powers of inquiry, including the power to summon witnesses, to formally require witnesses to testify under oath, and to provide requested information within specific deadlines.

635. The European Parliament must adopt a protocol for cases where member or staff of the House have become the direct or indirect target of spyware. All cases shall be reported to the responsible law enforcement authorities.

[989] Budget line 33 03 77 06, adopted in 2017.

Obtenu pour vous par
Got for you by
agence europe