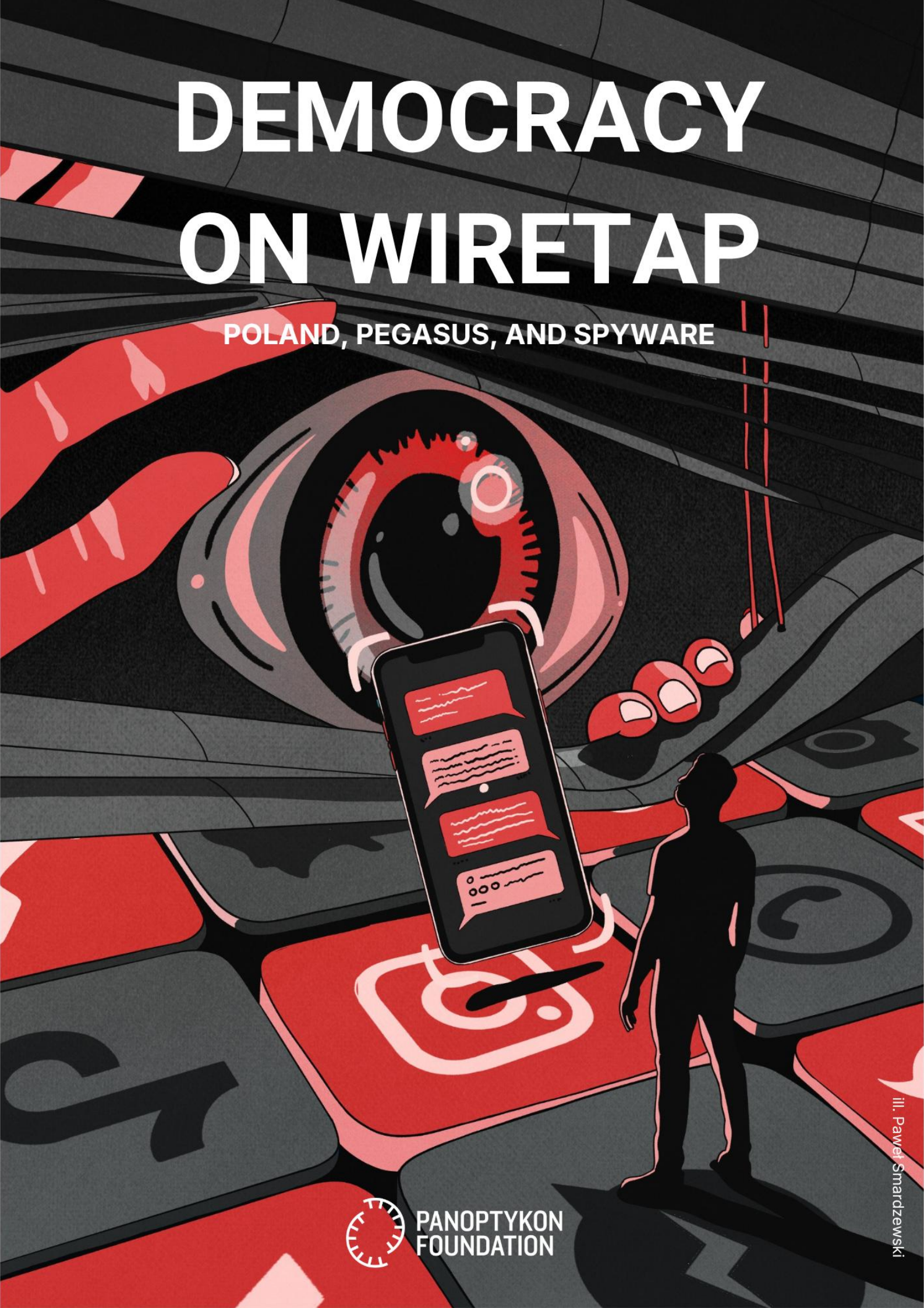
# DEMOCRACY ON WIRETAP

## POLAND, PEGASUS, AND SPYWARE



ill. Paweł Smardzewski

PANOPTYKON FOUNDATION

# Table of contents

# Introduction

**Spyware today is one of the most significant threats to democracy, human rights, and cybersecurity in the European Union and worldwide.**[1] For non-democratic governments it is one of the key tools used to maintain power and eliminate opponents: journalists, lawyers, opposition figures, and human rights defenders.

Spyware reaches through the ins and outs of a device – including through sensitive journalistic data, intimate correspondence with loved ones, online banking and social media activity. It allows for remote control of the microphone or camera. Used without scrutiny, spyware might very well be regarded as a 'nuclear weapon' stripping targets of all privacy.

Unscrutinised use of such technology poses a threat to the rule of law and civic engagement. It enables planting evidence and, consequently, framing people for crimes they did not commit or discrediting inconvenient journalists or activists. The Polish experience on the matter was particularly stringent. Between 2017 and 2022, Pegasus was used by authorities to spy on politicians: it provided the government with extraordinary insight into the opposition's plans. In fact, authorities went much further. As it will be detailed below, law enforcement authorities used spyware to extract 10 years of texts from one target, reorganised the texts and even merged some of them in order to rebuild a brand new narrative. This narrative was later sent to public TV and broadcasted, as part of a political smear campaign.

Despite multiple abuses having been exposed all over Europe, we are still learning about new cases of unauthorised use of spyware. Authoritarian regimes as well as democracies resort to it. They often deny using such tools – or admit to using them only after undeniable evidence has been revealed. At this stage we are not able to say whether Polish authorities still resort to such tools. However, it cannot be excluded.

**Why? Because the widely publicised promises of accountability and legislative changes have not been delivered.**

**Security services representatives argue that they need spyware to operate effectively.** Their main argument: the growing popularity of encrypted communication, which cannot be accessed with conventional methods of surveillance, such as retrieving phone records from telecom operators or the standard court-authorised wiretapping. This is

[1] EDRi, *Spyware and state abuse. The case for an EU-wide ban*, https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/.

why more than 100 countries around the world are now using – or independently developing – different types of spyware.[2]

Yet, spyware is like a nuclear weapon: it can determine the outcome of a war, while, at the same time, cause humungous damage. Politicians cannot ignore its existence any longer. A clear legal framework is necessary to prevent it from being used beyond scrutiny. Just as a nuclear weapon requires adequate safeguards for people's protection, spyware requires safeguards for civil rights and liberties.

This report examines why it is necessary both to conclude the 'Pegasus scandal' investigations, and to adopt legislation on spyware immediately. Poland needs to implement systemic changes to rules governing the judicial authorisation for an oversight over the use of surveillance techniques by the security services.

# Glossary

**Surveillance techniques** – covert surveillance of the activities of a person suspected of committing or planning a crime. Surveillance techniques may include wiretapping, accessing the content of correspondence (text messages, emails), mounting hidden cameras, inspecting postal items, and accessing data storage devices. They may be used by the police or the security services following authorisation by a prosecutor and a court.

**Spyware** – software that enables the collection of information about the user of an infected device, and transmits this information to third parties without the user's knowledge. In this report, we examine spyware used by state institutions.

**Secret services** – in Poland there are five secret (or intelligence) services: the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW), the Foreign Intelligence Agency (Agencja Wywiadu, AW), the Military Counterintelligence Service (Służba Kontrwywiadu Wojskowego, SKW), the Military Intelligence Service (Służba Wywiadu Wojskowego, SWW), and the Central Anti-Corruption Bureau (Centralne Biuro Antykorupcyjne, CBA). The Police, ABW, SKW, and CBA are authorised to use surveillance techniques. Other law enforcement agencies, such as the Military Police (Żandarmeria Wojskowa) and Border Guard (Straż Graniczna, SG) also use such techniques but less often that other agencies. We use term 'secret services' meaning all government agencies that carry out surveillance techniques.

[2] Share Foundation, *A privacy nightmare: understanding spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

# 1. Spyware

**In this chapter, we will examine:**

- Why spyware poses a threat to rights and freedoms that are the basis of democracy,
- What the 'Pegasus scandal' in Poland was about,
- How countries are currently abusing spyware.

## 1.1. How does spyware work

**Spyware usually enables a full view of the contents of an infected device.** It provides access to the correspondence exchanged via text messages and encrypted messaging apps, as well as to the contact list, emails, calendars, photos, recordings, social media, maps, music, film, and news apps, digital diaries, password managers, and everything else a person has on their device. It enables interception of phone calls and conversations conducted via instant messaging apps. This is known as the 'passive' function of spyware.


*A diagram from NSO Group's documentation illustrating the range of information that can be extracted from a device infected with Pegasus. Source: Hacking Team Emails/Citizen Lab, https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spy.*

**Some versions of spyware also allow the user to modify the contents of the device**, for example by saving and deleting files. This is known as the 'active' function.

**Like standard surveillance techniques, such as wiretapping, infecting a single device with spyware provides insight into the lives not only of the device owner, but also everyone else with whom they have ever communicated, if data was not deleted by the device's owner.**

It may take just one click on a malicious link to infect a device. This form of attack, known as one-click attack, was used against a Greek investigative journalist, whose phone was infected with Predator after he clicked on an innocent-looking link to a financial news website.[3] Similarly, an employee of Meta's Greek branch responsible for the company's cybersecurity policy was attacked – she clicked on a link posing as a confirmation of a doctor's appointment.[4]

There is even spyware that do not require any activity on the part of the target to be installed on their device. It is known as a zero-click attack. The infection of the device can occur for example through a missed WhatsApp call.[5] Spyware with a self-destruction function is also available on the market; it infects a phone without leaving any trace at all.[6]

## 1.2. Opposition politicians and female activists targeted

The most well-known spyware, Pegasus, first appeared in Poland in 2017.[7] The public first heard about it in 2018 following revelations by the Canadian university research unit

[3] Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, para. 207, https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2023/0189/P9_A(2023)0189_EN.pdf.

[4] Ibid., para. 232.

[5] Ibid., para. 286.

[6] Ibid., para. 494.

[7] This was not the first time the public had been made aware of evidence regarding the use of such tools by the Polish security services. In 2015, it emerged that the Central Anti-Corruption Bureau (CBA) had been a client of Hacking Team, a manufacturer of spyware. The invoices issued to the CBA related to the Remote Control System, used to infect and then remotely and covertly control devices such as computers and mobile phones.

Citizen Lab that the technology had been used in 45 countries, including Poland.[8] The use of Pegasus by the Central Anti-Corruption Bureau was brought to light by Adam Haertle, editor-in-chief of the Zaufana Trzecia Strona website, and Robert Zieliński, an investigative journalist at TVN24.pl.

Pegasus was used, among others, against the politician Krzysztof Brejza, the lawyer Roman Giertych, the prosecutor Ewa Wrzosek, as well as one of the leaders of the All-Poland Women's Strike, Klementyna Suchanow, and judge Beata Morawiec.

**In April 2024, the then Minister of Justice and Prosecutor General, Adam Bodnar, announced that between 2017 and 2022, three agencies had used 'surveillance of end devices' (i.e. used Pegasus software) on a total of 578 individuals.**[9] The list of those under surveillance was said to include 'far more public figures than have been revealed so far'.[10]

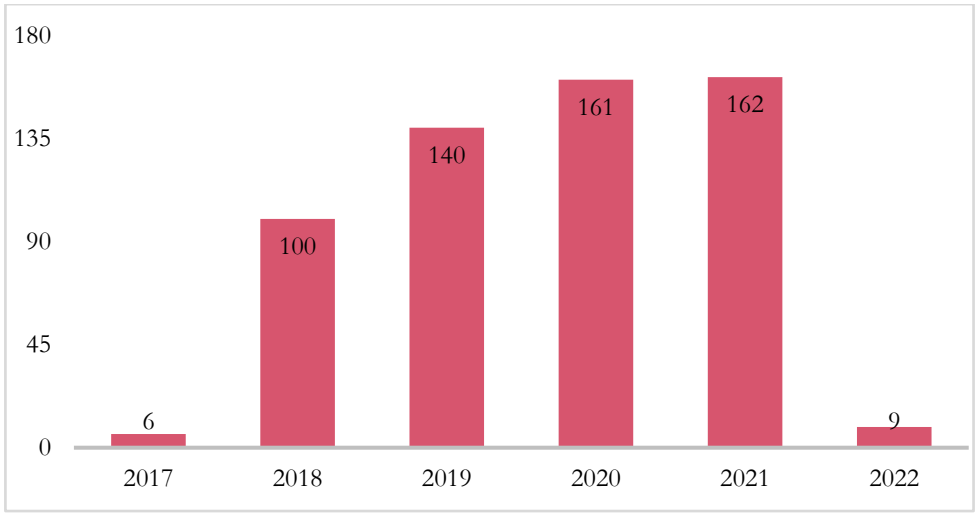



*Figure 1. People targeted with Pegasus in Poland between 2017 and 2022, according to Justice Minister.*

The main user of Pegasus in Poland was the Central Anti-Corruption Bureau, a law enforcement agency established to investigate corruption-related offences. This sets us apart from other countries, like Spain and Hungary, where the use of spyware was justified by threats to national security.

---

[8] Citizen Lab, *HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[9] Information on the total number of individuals against whom a request was made for the interception and recording of communications or for the authorisation of surveillance control in 2023, https://orka.sejm.gov.pl/Druki10ka.nsf/0/7522A4519FE790ACC1258B01003A2A38/%24File/308.pdf.

[10] The Guardian, *Poland launches inquiry into previous government's spyware use*, https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use.

According to information provided by Adam Bodnar, Pegasus was available to three agencies: the Central Anti-Corruption Bureau (CBA), the Internal Security Agency (ABW) and the Military Counterintelligence Service (SKW). It is also known that the Police used Pegasus, although it did not do so independently, but rather through the CBA. However, it is impossible to determine exactly how frequently each of the agencies used Pegasus.

At the time of writing this report, there is no information indicating that other agencies have used Pegasus.

In a report published in September 2023 on the work of the Special Committee appointed by the Senate in January 2022 to 'investigate cases of illegal surveillance, their impact on the electoral process in the Republic of Poland, and the reform of the secret services' (hereinafter 'the Senate Committee'), we find detailed information on attacks against public figures. We read that **civil society activists and entrepreneurs were also subject to spyware.**[11]

For example, the mobile phone of lawyer Roman Giertych (who represents, among others, PM Donald Tusk's family) was targeted at least 18 times. Agricultural community activist and a politician Michał Kołodziejczak was targeted 6 times. Entrepreneurs Paweł Tamborski and Andrzej Długosz were targeted in connection with the privatisation of the chemical manufacturing company CIECH – 5 and 61 times respectively.[12]

*Of all disclosed cases of device infection with Pegasus, the most high-profile and shocking is the case of politician Krzysztof Brejza. Brejza was the campaign manager for the Civic Coalition, which between 2015 and 2023 acted as the opposition party to the then-ruling Law and Justice party (PiS). The following data was stolen from the phone of Krzysztof Brejza, codenamed 'Grzechotnik' ('Rattlesnake') by CBA: 80,000 messages from 2010 to 2019, a set of keys containing all passwords to around 90 online services, full access to the location of placed phone-calls, emails, documents passing through his phones, photos, and video recordings.*[13]

During the 2019 election campaign, Mr. Brejza's phone was hacked at least 33 times, and the dates of these incidents coincide with key moments in the national campaign. It was

[11] Report of the Special Committee on the Investigation of Cases of Illegal Surveillance, Their Impact on the Electoral Process in the Republic of Poland, and the Reform of the Special Services, https://www.senat.gov.pl/download/gfx/senat/pl/defaultaktualnosci/1924/15764/1/raport_koncowy_z_prac_komisji_nadzwyczajnej.pdf.

[12] Ibid.

[13] Ibid.

CBA that used spyware against Mr. Brejza. Based on CBA operation documents, the Senate committee established that, all data extracted from his phone covered a period of nine years prior to the attacks.

The extracted data was later reorganized, some of the private text messages were merged and used to build a new narrative. It was then published in the Polish public media. This way, the ruling party used private information extracted via spyware to create a smear campaign against an opposition politician during an election campaign. In the context of the surveillance of Krzysztof Brejza, in 2019 Wojciech Hermeliński, former head of the National Electoral Commission and judge of the Constitutional Tribunal, told the Senate Committee:

> *The 2019 elections, while not rigged, were not fair.*[14]

In the cases examined by the Senate committee, none of the individuals targeted with spyware were eventually criminally charged. This would suggest that the surveillance was politically motivated rather than aimed at combating crime. MP Magdalena Łośko who, at the time of her being under Pegasus surveillance, served as assistant, coordinator, and office director to Krzysztof Brejza, told the Senate committee:

> *I was never charged with anything; those searches and the confiscation of electronic equipment were intended to discredit the Brejza family.*[15]

In November 2025, 38 people had been granted victim status in the prosecution's investigation into abuses involving the use of Pegasus software.[16]

Full information on the scale of Pegasus surveillance has not been made public and is unlikely ever to be.

[14] Bankier.pl, *Hermeliński: Wybory w 2019 roku, choć nie były sfałszowane, nie były uczciwe* [The 2019 elections, while not rigged, were not fair], https://www.bankier.pl/wiadomosc/Hermelinski-Wybory-w-2019-roku-choc-nie-byly-sfalszowane-nie-byly-uczciwe-8266533.html.

[15] Report of the Senate Committee, op. cit.

[16] Rzeczpospolita, *Adam Bodnar: Zbigniew Ziobro powinien trafić do aresztu. Zachodzi obawa mataczenia lub ucieczki* [Zbigniew Ziobro should be taken into custody. There is a risk that he might tamper with evidence or abscond], https://www.rp.pl/polityka/art43290211-adam-bodnar-zbigniew-ziobro-powinien-trafic-do-aresztu-zachodzi-obawa-mataczenia-lub-ucieczki.

## 1.3. How other countries have used (and continue to use) spyware

### 1.3.1. Italy: Surveillance of government's critics

In January 2025, WhatsApp sent a notification to around 90 Italian users of the app, informing them that they may have been targeted with the Graphite spyware. The software's developer, the Israeli company Paragon, claimed that its terms of service prohibited the unauthorised use of the product. However, in March 2026, the Italian public prosecutor's office confirmed that in 2024, two pro-immigration activists and an investigative journalist critical of Giorgia Meloni's government had been targeted.

Among those reportedly infected were a chaplain – a friend of the late Pope Francis – working on a rescue ship belonging to an organisation that rescues migrants in the Mediterranean, and a journalist from the Fanpage.it, who had exposed links between the Italian Prime Minister's party and neo-fascist circles. Journalist Ciro Pellegrino wondered:

> *Why have I become a target? I have been asking myself this question ever since I received the notification. I intend – and we intend – to put this question publicly to everyone who has the authority and the duty to answer it. An answer is owed to… everyone who is interested in knowing who in this country has blurred the clear line between security and surveillance, between legality and abuse.*[17]

A report published by the Italian parliamentary committee on security reveals that, between 2023 and 2024, Italian intelligence services had contracts in place with the company, Paragon.[18] It remains unclear who commissioned the surveillance.

[17] The Guardian, *Second Italian journalist allegedly targeted with 'mercenary spyware'*, https://www.theguardian.com/world/2025/may/01/second-italian-journalist-allegedly-targeted-with-mercenary-spyware.

[18] Citizen Lab, *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*, https://citizenlab.ca/research/a-first-look-at-paragons-proliferating-spyware-operations/#h-3-whatsapps-paragon-investigation.

### 1.3.2. Serbia: Digital prison

According to Citizen Lab, the Serbian Information Security Agency (BIA) has used various commercial spyware tools through the years, for example FinFisher from the German company FinFisher GmbH (2014),[19] products from Circles, a company linked to the NSO Group (2020),[20] and Predator from Cytrox, a member of the Intellexa consortium (2021).[21] Since at least December 2021, Serbia has also been using Pegasus, including to surveil civil society representatives critical of the Serbian government (2023).[22]

In 2024, Amnesty International revealed the use of a spyware called NoviSpy. Expert findings indicate that this new, locally developed software was used by state authorities against journalists and activists. Amnesty International described the overall pattern of surveillance and repression against civil society in Serbia as a 'digital prison'. NoviSpy enabled authorities to infect a device only through direct physical contact. The software was installed for example during anti-government demonstrations, when the protesters were in custody and their devices were in the hands of the authorities.[23]

### 1.3.3. Greece: The first convictions

Between 2021 and 2022 the spyware called Predator, developed by the Intellexa group, was used in Greece to monitor the phones of around 90 people.[24] This international consortium is one of the main competitors of the NSO Group, the developer of Pegasus.

---

[19] Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

[20] Citizen Lab, *Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles*, https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

[21] Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[22] Access Now, *Spyware in Serbia: civil society under attack*, https://www.accessnow.org/spyware-attack-in-serbia/.

[23] Amnesty International, *Serbia: 'A Digital Prison': Surveillance and the suppression of civil society in Serbia*, https://www.amnesty.org/en/documents/eur70/8813/2024/en/.

[24] International Consortium of Investigative Journalists, *Greek court convicts Intellexa founder Tal Dilian, three others in wiretapping scandal*, https://www.icij.org/investigations/cyprus-confidential/greek-court-convicts-intellexa-founder-tal-dilian-three-others-in-wiretapping-scandal/ and Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

It operates from Greece and – according to the company itself – is 'subject to EU regulations'.

Those targeted by the surveillance included a financial journalist, opposition politicians, an Member of the European Parliament (MEP), ministers, intelligence agents, prosecutors and the former Head of Trust and Safety at Meta. The revelation of the case led to a political crisis and the resignation of Greek intelligence service's head, together with one of the prime minister's closest aides.

In February 2026, a court of first instance sentenced four members of Intellexa's management to a total of 126 years in prison, although they will actually serve a maximum of eight years, and the sentence has been suspended pending the outcome of the appeal.[25] Convictions may lead to further criminal proceedings against those involved in the scheme, as well as espionage charges.

### 1.3.4. United Kingdom/Saudi Arabia: Compensation for surveillance

Ghanem Al-Masarir, a London-based Saudi human rights activist and a popular political satirist on YouTube, was among those targeted by the Saudi operator of Pegasus in 2018. The activist sued the Kingdom of Saudi Arabia, seeking compensation and damages for emotional distress and loss of earnings. A British court ruled in his favour and, in January 2026, ordered Saudi Arabia to pay £3 million for, among other things, the pain, suffering, and loss of quality of life he had endured, as well as the damages and lost earnings he had suffered.[26]

It is not known whether Saudi Arabia will pay the claimant the sum awarded, but according to Al-Masari – regardless of the outcome of the court proceedings and whether the compensation is paid – the Saudi government has achieved its goal, which was to block his satirical online activity:

---

[25] The Record, *Intellexa founder, three others sentenced to 8 years in prison over Greek spyware scandal*, https://therecord.media/spyware-intellexa-greece-sentenced and Ekathimerini.com, *Four businesspeople found guilty in 2022 spyware scandal*, https://www.ekathimerini.com/news/1296353/four-businesspeople-found-guilty-in-spyware-trial/.

[26] Judgment in the case of Ghanem Al-Masarir v. the Kingdom of Saudi Arabia, https://caselaw.nationalarchives.gov.uk/ewhc/kb/2026/119 and Citizen Lab, *Saudi Arabia Ordered to Pay £3m to London Dissident Over Pegasus Spying*, https://citizenlab.ca/saudi-arabia-ordered-to-pay-3m-to-london-dissident-over-pegasus-spying/.

*I hope they will comply and pay the debt as soon as possible. If they don't pay it, we won't have any other alternative but to take enforcement action to recover the money from Saudi assets abroad, it doesn't have to be the UK.*

*It's a win for them because they silenced me and I'm not able to do my work anymore.*[27]

***

According to a report compiled by the Serbian Share Foundation, nearly 100 countries worldwide use one of the many commercial spyware programs (so-called 'mercenary spyware') or are developing their own tools of this kind.[28] The use of the Pegasus spyware in Poland therefore fits into a broader international context. In the next section, we will examine the arguments for and against the claim that the use of this technology by security services is lawful.

# 2. Arguments against the legality of Pegasus

**In this chapter, we:**

- Dismantle arguments put forward by those who support the view that the use of spyware in Poland is lawful; and
- Explain how the use of spyware violates EU law.

## 2.1. Spyware does not fall within the legal definition of surveillance techniques

Surveillance techniques may involve, amongst other things, 'obtaining and recording data contained in data storage devices, telecommunications end devices, and IT and ICT systems'.[29]

[27] The Guardian, *Saudi dissident awarded £3m damages threatens enforcement action if he is not paid*, https://www.theguardian.com/world/2026/jan/30/saudi-dissident-awarded-3m-damages-threatens-enforcement-action-if-he-is-not-paid.

[28] Share Foundation, *A Privacy Nightmare: Understanding Spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

[29] In accordance with Article 17(5)(4) of the Act on the Central Anti-Corruption Bureau. Similar provisions apply to other services.

That is precisely what spyware is for – at least according to **those who maintain that Pegasus is legal. They regard it as a surveillance technique like any other.**

This interpretation appears to be supported by the Supreme Court's resolution of 23 April 2023. According to this resolution, the provisions governing the activities of the security services specify 'the types of information or data that may be obtained through surveillance techniques, rather than specifying the particular technical means'.

---

*It seems that in an era of rapid technological progress, it is not possible to list such technical means in the resolution. For example, there has been development in the area of so-called spyware, which does not require cooperation with a mobile network operator and, by 'infecting phones', allows for the copying of sent or received messages, the collection of photos, the recording of conversations, activating the microphone to eavesdrop on conversations, activating the camera to record what is happening around a person, enabling access to so-called 'historical' data — i.e. from the period prior to the installation of such software —and featuring a 'self-destruct' option, meaning it leaves no traces on the 'infected' device.*[30]

---

**One argument against this interpretation is that the use of Pegasus and other spyware involves bypassing the device's security measures and altering the way it operates.** Neither the Act on the Central Anti-Corruption Bureau nor any other legislation grants secret services the right to bypass the security measures on devices belonging to individuals who are subject to surveillance.

This was confirmed by the Wrocław Court of Appeal, in its ruling of 11 May 2023, which excluded evidence obtained using Pegasus and consequently acquitted an officer accused of disclosing classified information.

[30] Resolution of the Supreme Court of 26 April 2023, ref. no. I ZI 50/22, https://www.sn.pl/sites/orzecznictwo/orzeczenia3/i%20zi%2050-22.pdf.

*Software such as spyware grants full access to a mobile device, enabling data to be retrieved and stored. The problem, however, is that it is installed by circumventing and breaching security measures – effectively hacking into the phone – in a way that compromises its structure. Meanwhile, the current regulations on surveillance techniques, including the aforementioned Article 17 of the Act on the Central Anti-Corruption Bureau, do not permit such actions and do not provide for such a possibility.*[31]

**Secondly, spyware makes it possible to collect and store historical data – including data from the period prior to the decision to order surveillance** and without any time restrictions, provided the data is available. Meanwhile, the court may order surveillance for a maximum of three months from the date the surveillance is ordered, but not retroactively.

As General Krzysztof Bondaryk explained:

*Surveillance techniques are used in real time and are oriented towards the future; in other words, from today onwards, for a period of three months, you or I may be listened to, rather than, for example, for four years looking back from today.*[32]

This means that the retrieval in 2019 of 80,000 messages from the period 2010–2019 from a mobile phone belonging to Krzysztof Brejza[33] also did not fall within the current legal definition of surveillance techniques.

The Wrocław Court of Appeal also highlighted this issue in the aforementioned judgment. Interpreting the provisions of the Act on the Central Anti-Corruption Bureau (CBA) in the light of the Constitution, the court concluded that:

[31] Judgment of 11 May 2023, ref. no. II AKa 480/21, https://www.saos.org.pl/judgments/501168.

[32] Session of 12 February 2026, https://sejm.gov.pl/Sejm10.nsf/biuletyn.xsp?skrnr=SKPG-126. We discuss the work of the Sejm Inquiry Committee in more detail in section 3.6.

[33] Report of the Special Committee on the Investigation of Cases of Illegal Surveillance, Their Impact on the Electoral Process in the Republic of Poland, and the Reform of the Special Services, https://www.senat.gov.pl/download/gfx/senat/pl/defaultaktualnosci/1924/15764/1/raport_koncowy_z_prac_komisji_nadzwyczajnej.pdf.

*it is unacceptable for the services to use such surveillance techniques which involve (...) gaining access to a wide range of data, including historical data, which goes beyond the time frame of the authorised surveillance (...), the use of spyware cannot be regarded as a legal means of obtaining such data in accordance with the Act.*

**Thirdly, spyware provides access not only to data stored on the device, but also to apps and their history.** It allows the secret services to view the feed of any app, access the target's online banking, or view their purchase history on Vinted.

**Therefore, in our view, there is currently no legal basis in the legislation to consider that Pegasus or other spyware fits into the current legal definition of surveillance techniques.**

## 2.2. The courts have no real control over the activities of the security services

**The second argument in favour of Pegasus's legality is the judicial oversight** of the security services' surveillance activities. Adam Bodnar, in his capacity as Minister of Justice and Prosecutor General, confirmed in the Sejm that there had been no instances of Pegasus being used without court authorisation.

We have no grounds to question this statement. **It is, however, quite possible that in none of the 578 cases was the court aware that it was authorising the use of spyware.** As Igor Tuleya, a judge at the Regional Court in Warsaw, said in an interview with Rzeczpospolita:

*It is very likely that I authorised the use of Pegasus without realising what system would actually be used.*[34]

Marzanna Piekarska-Drążek, a judge at the Court of Appeal in Warsaw, testified before the Sejm Investigation Committee as follows:

[34] Rzeczpospolita, *Sędzia Igor Tuleya: Możliwe, że zgodziłem się na Pegasusa* [Judge Igor Tuleya: It is likely that I authorised the use of Pegasus], https://www.rp.pl/sady-i-trybunaly/art39874451-sedzia-igor-tuleya-mozliwe-ze-zgodzilem-sie-na-pegasusa.

*In the case of the use of surveillance techniques such as Pegasus, it is difficult to reconcile this with the provisions of the law, because no one anticipated that such a system would be used legally, that is, within the framework of existing law. No one foresaw this.*[35]

Piotr Gąciarek, a judge at the Regional Court in Warsaw, stated before the Senate Committee:

*In my opinion – based on what we already know about this intrusive tool Pegasus and on the current state of law (...) – I believe it was not possible for the court to consciously authorise surveillance with the use of Pegasus. I rule out such a possibility. If Pegasus was used, in my opinion the authorisation was obtained by deception – by not naming the surveillance technique to be used in a straightforward way.*[36]

Withholding information from the judges' is a part of a wider problem concerning the inadequacy of judicial oversight of the use of surveillance techniques. A problem which was examined by the European Court of Human Rights in the case of Pietrzak, Bychawska-Siniarska, and Others v. Poland. The Court held that 'judicial authorisation (...) is a very useful procedural safeguard, but is not sufficient in itself'. The ruling also confirms that there is no real and effective mechanism in Poland for supervising the use of surveillance techniques. So then, what is the nature of its flaw?

**Firstly, while applying for judicial authorisation of surveillance, secret services present only the materials that 'justify' the need of it – not the full dossier on the target.** As Dr Adam Behan, an adviser to the Sejm Inquiry Committee, points out:

*This allows the services to 'sidestep' inconvenient facts, context, or even circumstances that suggest that a given person has no connection to the case, and which – were they included in the submitted documents – could result in judicial authorisation not being granted.*[37]

[35] Session of 12 September 2025, https://sejm.gov.pl/Sejm10.nsf/biuletyn.xsp?skrnr=SKPG-102.

[36] Session of 27 January 2023, https://www.senat.gov.pl/prace/komisje-senackie/przebieg,10026,1.html.

[37] Prawo.pl, *Kontrola operacyjna wymknęła się... spod kontroli* [Surveillance got... out of control], https://www.prawo.pl/prawnicy-sady/sedziowie-nie-moga-byc-manipulowani-przez-sluzby,525859.html.

**Secondly, proceedings concerning the authorisation of surveillance do not involve a party representing the right to privacy of the person who will be subject to the surveillance** (e.g. the so-called 'privacy advocate' familiar from the British model). Only security services and the prosecutor take part in proceedings. Therefore, if the court grants authorisation for specific surveillance techniques, there is no one to challenge the validity of that decision on either legal or technical grounds.

**Thirdly, only refusals to authorise surveillance require a statement of reasons.** This acts as a kind of incentive for judges to grant authorisation for such measures. The Civic Coalition government attempted to impose an obligation on the courts to provide reasons for granting authorisation for surveillance as well, but did so by means of regulations, rendering this change ineffective (see 3.5.1.).

**Fourthly,** even without the need to provide statements of reason in case of granting authorisation judges struggle with capacity. In fact, **applications are considered by just one (!) judge on duty that day,** who is expected to review several dozen applications for surveillance authorisation within one or two days.[38]

Consequently, courts grant authorisation for surveillance techniques requests in over 99% of cases (see Table 1).

However, according to Dr Dominika Czerniak of the Office of the Ombudsman, the conditions under which judges consider requests from security services 'do not justify an opportunistic approach to the right to privacy or the *rubber-stamping* of requests'.[39]

It remains a matter of debate, whether judges already have effective tools at their disposal to scrutinise requests from security services (but fail to use them), or the problem lies in flawed regulations. Nevertheless, under the current model, judicial review does not provide protection against abuses – neither in the case of conventional surveillance techniques nor in the use of spyware.

---

[38] The Regional Court in Warsaw receives an average of around 25 requests to authorize surveillance every day – including Sundays and public holidays. Office of the Ombudsman, *Implementation of the judgment of the European Court of Human Rights in the case of Pietrzak and Bychawska-Siniarska and Others v. Poland (case nos. 72038/17 and 25237/18). Report on necessary amendments to the regulations governing the extrajudicial and judicial monitoring and recording of conversations,* https://bip.brpo.gov.pl/sites/default/files/2025-11/Raport_wykonanie_wyroku_etpc_inwigilacja_3_07_2025.pdf.

[39] Ibid.

| Year | Requests from the security services | Refusal by the prosecutor | | Approval by the prosecutor (requests are forwarded to the court) | | Refusal by the court (no surveillance carried out) | | Approval by the court (the services carry out surveillance) | |
|---|---|---|---|---|---|---|---|---|---|
| | Number of people | Number of people | % | Number of people | % | Number of people | % | Number of people | % |
| 2024 | 5818 | 95 | 1,63% | 5723 | 98,37% | 26 | 0,454% | 5697 | **99,55%** |
| 2023 | 5973 | 116 | 1,94% | 5857 | 98,06% | 22 | 0,376% | 5835 | **99,62%** |
| 2022 | 6381 | 129 | 2,02% | 6252 | 97,98% | 38 | 0,608% | 6214 | **99,39%** |
| 2021 | 7071 | 126 | 1,78% | 6945 | 98,22% | 25 | 0,360% | 6920 | **99,64%** |
| 2020 | 6537 | 118 | 1,81% | 6419 | 98,19% | 35 | 0,545% | 6384 | **99,45%** |
| 2019 | 5839 | 103 | 1,76% | 5736 | 98,24% | 25 | 0,436% | 5711 | **99,56%** |
| 2018 | 6088 | 148 | 2,43% | 5940 | 97,57% | 25 | 0,421% | 5915 | **99,58%** |
| 2017 | 6562 | 146 | 2,22% | 6416 | 97,78% | 14 | 0,218% | 6402 | **99,78%** |

*Table 1. Despite the 'Pegasus scandal', courts continue to approve over 99% of applications for surveillance. Source: Panoptykon's analysis based on the annual reports of the Prosecutor General.*

## 2.3. Spyware as a threat to national security

Pegasus has never been granted ICT security accreditation by the Internal Security Agency (ABW), which is required for systems used to process classified information. However, according to Colonel Przemysław Leśniak, former Director of the ABW's Classified Information Department, 'Pegasus is not an ICT system and does not process classified information.[40] As such, in his opinion, it did not require the aforementioned accreditation.

However, the National Public Prosecutor's Office stated that the Pegasus system should be subject to ICT security accreditation, yet it never obtained one'.[41] This means that the software in question might have leaked the information regarding our intelligence services' operation interests to third parties (e.g. employees of NSO Group and Israeli

[40] Colonel Przemysław Leśniak's profile on X, https://x.com/przemkolesniak/status/2029262770776977767.

[41] The accreditation requirement stems from Article 48 of the Act on the Protection of Classified Information, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228. The National Public Prosecutor's Office, *ABW: the Pegasus system should be subject to ICT security accreditation*, https://www.gov.pl/web/prokuratura-krajowa/abw-system-pegasus-powinien-podlegac-akredytacji-bezpieczenstwa-teleinformatycznego.

intelligence services).[42] It might have provided unauthorised access to data to a foreign software manufacturer.[43] This effectively means that Polish intelligence services could have been spied upon.

This claim was confirmed by a declassified internal document from the Military Counter Intelligence Service obtained by the Sejm Inquiry Committee. The document reportedly contained a warning that 'the system in use **does not rule out the possibility of the software manufacturer accessing the transmitted data**'.[44]

The findings contained in the Military Counterintelligence Service document corroborate the information disclosed by Adam Haertle, editor-in-chief of Zaufana Trzecia Strona, according to which Pegasus used the Pegasus Anonymizing Transmission Network (PATN) – **a network of NSO-controlled servers scattered across the globe – to transmit data.**[45] This means that **information obtained via this software left the infrastructure controlled by the licensee (e.g. the CBA) and was sent to the software manufacturer**.

Neither those under surveillance nor the Polish authorities have any means of verifying what happened to the data that reached the Pegasus manufacturer, or how it will be used in the future. Importantly, this problem stems from a short-sighted decision to purchase a third-party software licence rather than the software itself.

## 2.4. Spyware breaches EU law

The European Union also opposes the use of spyware under current legislation. The European Parliament's PEGA Committee, set up to investigate the use of Pegasus in European Union countries, including Poland, has concluded that it contravenes EU law.

**Firstly, it infringes on the Charter of Fundamental Rights of the European Union (CFR).** By allowing full, covert control over devices, it infringes Articles 7 (the right to respect for one's private life) and 8 (the right to the protection of personal data) of the CFR. In

---

[42] Spider's Web, *Pegasus jest jeszcze bardziej nielegalny, niż się wydawało* [Pegasus is even more illegal than previously thought], https://spidersweb.pl/2025/05/pegasus-nie-mial-akredytacji-bezpieczenstwa.html.

[43] TVN24, *Kluczowy dokument na biurku w prokuraturze. Wszystkie dane mogły trafiać do Izraela* [Key document on a desk at the prosecutor's office. 'All data could have ended up in Israel'], https://tvn24.pl/polska/pegasus-kluczowy-dokument-z-abw-na-biurku-w-prokuraturze-wszystkie-dane-mogly-trafiac-do-izraela-st9159963.

[44] Magdalena Sroka, Chair of the Sejm Inquiry Committee, referred to this document during the session on 27 June 2026.

[45] Zaufana Trzecia Strona, *5 powodów, dla których używanie Pegasusa w Polsce nie mogło być legalne* [5 reasons why using Pegasus in Poland could not have been legal], https://zaufanatrzeciastrona.pl/post/5-powodow-dla-ktorych-uzywanie-pegasusa-w-polsce-nie-moglo-byc-legalne/.

accordance with Article 52 of the Charter and the established case law of the Court of Justice of the European Union, any interference with fundamental rights must meet the requirements of legality, necessity, and proportionality. Meanwhile, Pegasus – given the scope of its capabilities – can easily lead to interference exceeding what would be considered proportionate in a democratic state governed by the rule of law, for instance due to access to historic data, as mentioned above. The ability to interfere with the data on the target device also undermines the fundamental guarantees of a fair trial (Article 47 of the CFR), calling into question the admissibility of evidence in court.

The PEGA Committee also highlights the abuse by Member States of the 'national security' clause (Article 4(2) of the Treaty on European Union). In its view, this cannot serve as a justification for disregarding fundamental rights. Case law of the EU's top court, the Court of Justice of the European Union (CJEU) clearly indicates that considerations of national security do not justify unlimited infringements of fundamental rights.[46]

**Secondly, the use of Pegasus may breach the General Data Protection Regulation (GDPR).** When used without proper oversight, spyware can lead to the processing of personal data on a massive scale, without the knowledge or consent of the data subject, and without complying with fundamental processing principles such as data minimisation and purpose limitation.

**Thirdly, it breaches the ePrivacy Directive** (Directive 2002/58/EC), which establishes the principle that the interception of electronic communications and access to information stored on a user's device are permissible only with their consent or on the basis of strictly defined exceptions (i.e. national security, suspicion of a criminal offence). Meanwhile, the very nature of spyware is to gain such access without the user's knowledge or consent. We know, however, that many instances of spyware use were unrelated to either national security or a legitimate fight against crime.

Among the recommendations formulated by the European Parliament was a call for the development of EU legislation to regulate the use of spyware by the authorities of Member States.[47]

***

[46] See ruling of the grand chamber of the Court of justice in case C-511/18 – La Quadrature du Net and Others, para. 190-191. See Data Rights, *Takeaways from Data Rights about the CJEU rulings 'Privacy International' and 'La Quadrature du Net, French Data Network et al.'*, https://data-rights.odoo.com/takeawayslqdn2020ruling.

[47] European Parliament recommendation of 15 June 2023 to the Council and the Commission following an inquiry into allegations of breaches of Union law and maladministration in its application in relation to Pegasus and equivalent spyware (2023/2500(RSP)), paragraph 32.

On the one hand, there are the security services arguing that they need tools such as Pegasus, and those who support its use on the grounds that it is legal. On the other: an unresolved scandal, numerous arguments challenging the claim that the tool is legal, and fears of a drastic curtailment of rights and freedoms. This dispute demonstrates that we urgently need legislation.

In the next section, we will look at what has happened in Poland since the first cases of Pegasus's use by the security services were uncovered. Why do we refer to the 'Pegasus scandal'? What lessons have we learnt from it, and what has changed in Poland since the surveillance was exposed?

# 3. What has changed in Poland since the 'Pegasus scandal'?

**In this chapter, we will:**

- Look back at the reactions of politicians to the exposed abuses, and at the promises they made during the campaign,
- Summarise the actions that have been taken,
- Examine whether anyone has been held to account for the abuses.

## 3.1. Announcements regarding the introduction of oversight of security services

In 2023, Poland was in the midst of a parliamentary election campaign. Pegasus and its illegal use by security services were among topics of the campaign. Donald Tusk , then leader of the opposition and now Prime Minister, even proposed a reworked meaning of the then ruling Law and Justice party, acronym from the original 'Law and Justice' [Prawo i Sprawiedliwość] to 'Bribery, Surveillance, Blackmail' [Przekupstwo Inwigilacja Szantaż]. While criticising the PiS party, **politicians from the Civic Coalition, as well as other opposition groups, declared the need for changes in security services' oversight.** This would, understandably, cover their use of spyware.

During the Civic Coalition's '100 Specifics' Congress in September 2023, Krzysztof Brejza declared:

*We will ensure the security of your phones and your correspondence (...), and each of you will be able to submit a written enquiry asking whether you have been under surveillance.*[48]

He was not the only one. Radosław Sikorski, MEP at the time, also attempted to gain electoral capital on the promise of oversight of security services:

The campaign pledges were translated into concrete provisions in the coalition agreement between the parties currently forming the government (Civic Coalition, New Left, Polish Coalition – Poland 2050 and Polish Coalition – PSL). **Point 19 of the agreement provided, amongst other things, for the introduction of an effective mechanism to oversee the use of surveillance techniques by security services, and for granting citizens the right to information regarding the security services' interest in them, in particular information about any surveillance techniques measures being used against them.**[49]


*'If you don't want the authorities to be able to eavesdrop on anyone who opposes the government, vote for KO' – Radosław Sikorski posted an election poster with this message on his X profile on 12 October 2023. The post was tagged with the hashtags (translated): #Pegasus # PiSScandals #Surveillance #PiSIsEvil #PiSIsAShame #PolandInOurHearts, https://x.com/sikorskiradek/status/1712440684542599541.*

[48] Donald Tusk – official YouTube channel, *Donald Tusk: Kongres 100 konkretów, Tarnów, 9.09.2023* [Donald Tusk: The '100 Specifics Congress, Tarnów, 9 September 2023]; Krzysztofa Brejza appears at 1:02:11, https://www.youtube.com/live/rLzOWVm3epo?t=3720s.

[49] Coalition Agreement of 10 November 2023, https://platforma.org/upload/document/203/attachments/433/UmowaKoalicyjna.pdf.

In addition to this provision, the coalition agreement addressed the issue of using surveillance techniques by security services at length. We therefore anticipated that the rules governing the use of spyware such as Pegasus would soon be regulated.

Yet, to date, we have not seen these promises fulfilled.

## 3.2. The Senate Special Committee recommends changes

Just over a month before the elections, on 6 September 2023, the Senate Special Committee concluded its investigation of cases of illegal surveillance, their impact on the electoral process in the Republic of Poland, and the reform of security services.

The Senate Committee did not have the powers of an inquiry committee. It was established while the Law and Justice (PiS) party was in government. The creation of a committee was only possible because, at the time, the opposition had a majority in the Senate: all its members were affiliated with parties that currently form the government. The committee chair, Marcin Bosacki, is now Deputy Minister for Foreign Affairs.

In its final report, the committee recommended systemic changes to the oversight of security services. In particular, it emphasised the need to clearly state that the modification of data obtained through advanced surveillance techniques is unacceptable, and the need to introduce a notification requirement, i.e. granting individuals the right to be informed that they were the subject of surveillance.

Three years have passed, but the changes still have not been implemented.

## 3.3. Code of Operational Procedure: a discarded proposal for oversight of security services

In 2023, a draft act—the Code of Operational Procedure— was drawn up within secret services community, with the active involvement of General Krzysztof Bondaryk (head of the Internal Security Agency from 2007 to 2013). The Code was intended to comprehensively regulate and organise matters relating to surveillance techniques used by security services.

The draft act legalised the use of spyware. It permitted 'covert interference' involving 'the covert access to telecommunications-end devices and IT and ICT systems, with the aim of obtaining and recording the data contained therein'.[50]

[50] Draft Act on the Code of Operational Procedure of 17 April 2023, https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf.

At the same time, the act strengthened the mechanism of judicial oversight over the activities of security services, in relation to using surveillance techniques and spyware. It also imposed an obligation on the head of the service conducting the surveillance to inform the person subject to 'covert interference' of the fact that it had taken place – no later than 12 months after the interference had ended.

Following the 2023 elections, work on the Code of Operational Procedure was abandoned.

## 3.4. Ruling of Pietrzak, Bychawska-Siniarska and others v. Poland – reforms are a 'priority' for the government

On 28 May 2024, more than six months after the new coalition formed a government, the European Court of Human Rights (ECtHR) delivered its judgment in the case of Pietrzak, Bychawska-Siniarska and Others v. Poland.

The case, initiated in 2019 by activists from the Panoptykon Foundation (Katarzyna Szymielewicz and Wojciech Klicki), the Helsinki Foundation for Human Rights (Dominika Bychawska-Siniarska and Barbara Grabowska-Moroz), and lawyer Mikołaj Pietrzak, concerned a wide range of issues relating to the rules governing the use of surveillance techniques by Polish security services and judicial oversight of their activities. It did not directly concern spyware. Spyware – as we argue in section 2.1 – goes beyond the current legal definition of surveillance techniques. However, the security services have so far followed a different interpretation. That is why we analyse here the promises and proposals concerning the notion of surveillance techniques in general – see 3.5.).[51]

The ECtHR found that the system of oversight over the use of surveillance techniques by Polish security services – despite theoretical judicial oversight – does not protect against abuses (see section 2.3).

[51] Panoptykon Foundation, *Inwigilacja w Polsce narusza twoje prawa. Ważny wyrok Europejskiego Trybunału Praw Człowieka* [European Court of Human Rights: secret surveillance in Poland violates citizens' privacy rights], https://panoptykon.org/wyrok-ETPC-inwigiliacja-2024.

The judgment was to become – as Minister of Justice Adam Bodnar stated – 'a significant impetus for further action'. As Minister Coordinator of Special Services Tomasz Siemoniak added, its implementation was to be 'one of the government's priorities'.[52]

Yet, at the time of publication of this report, the ruling has not been implemented.

## 3.5. Insufficient legislation changes

In 2024, the government adopted **a series of regulations amending the rules governing surveillance techniques** by the Police, the Internal Security Agency, and other security services.[53] Towards the end of 2025, work began on **a draft act amending certain acts 'to strengthen judicial oversight of the use of** surveillance techniques'.[54]

### 3.5.1. Ineffective regulations

The regulations introduce two amendments:

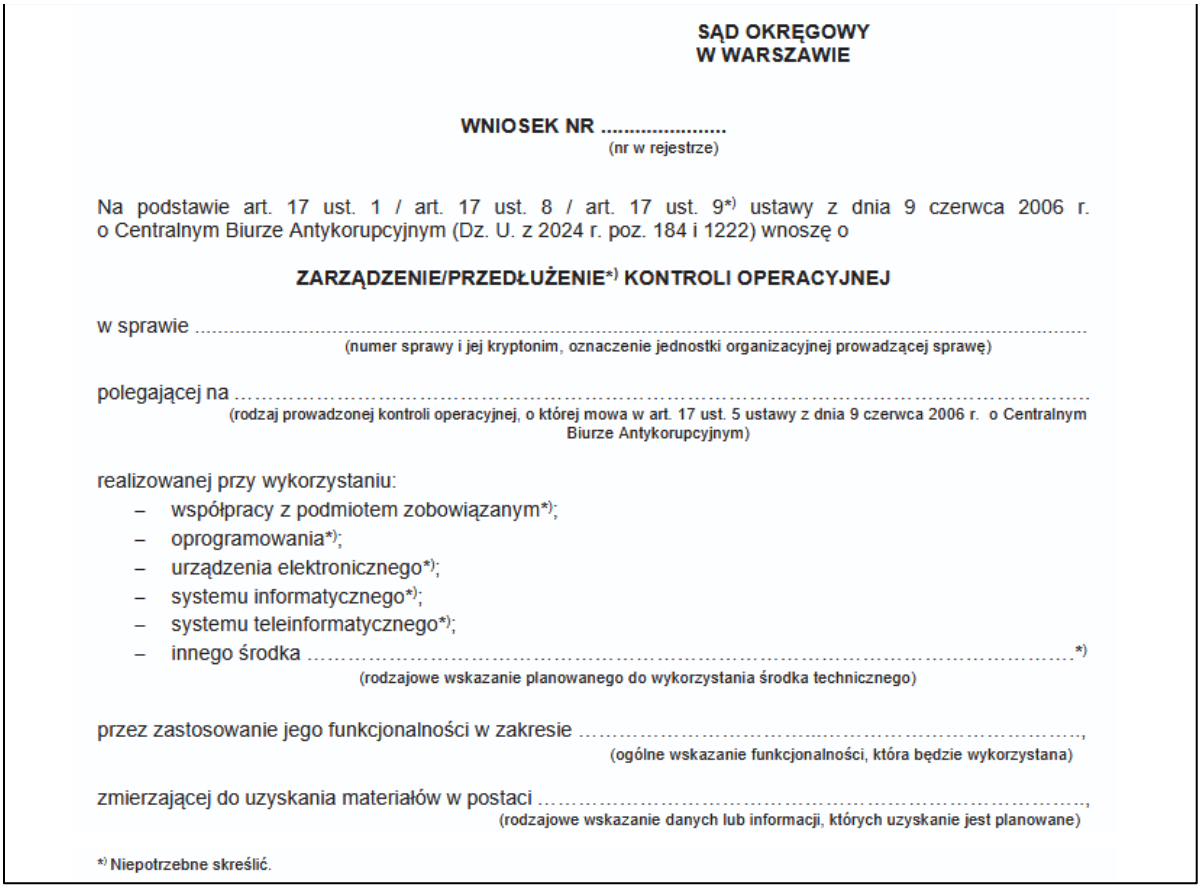
1) In the statement of reasons accompanying an application to the court for authorisation of the use of surveillance, the security service should specify what technique it intends to use and what type of data it intends to obtain through it. This ensures that the court knows, for example, whether a 'traditional' wiretapping or spyware is to be used;
2) The court must provide reasons for both granting and refusing authorisation for surveillance. This was intended to reduce the likelihood of courts automatically accepting applications, as well as to implement one of the recommendations of the ECtHR in the above-mentioned case of Pietrzak, Bychawska-Siniarska and Others v. Poland.

[52] Ministry of the Interior and Administration, *Konferencja prasowa dotycząca orzeczenia ETPC ws. kontroli operacyjnej w Polsce* [Press conference on the ECtHR ruling regarding the use of surveillance techniques in Poland], https://www.gov.pl/web/mswia/konferencja-prasowa-dotyczaca-orzeczenia-etpc-ws-kontroli-operacyjnej-w-polsce, and a recording from the conference (from the 7th minute), https://www.youtube.com/watch?v=ylXp7h0k56A.

[53] Panoptykon Foundation, *Wzmocniona kontrola nad działaniami Krajowej Administracji Skarbowej – projekt opublikowany po apelu organizacji* [Tighter oversight of the National Revenue Administration's activities – draft regulation published following an appeal by the organisation], https://panoptykon.org/krajowa-administracja-skarbowa-po-apelu.

[54] Draft act amending certain acts to strengthen judicial oversight of the use of surveillance techniques, https://sejm.gov.pl/Sejm10.nsf/druk.xsp?documentId=63F5DE808433ECBCC1258DD90031980F, at the time of writing, Sejm deliberations on the draft were ongoing.

The first of these amendments is unequivocally positive: any change that increases the amount of information available to judges has a positive impact on their ability to exercise effective oversight over the activities security services wish to carry out.



SĄD OKRĘGOWY
W WARSZAWIE

**WNIOSEK NR .....**
(nr w rejestrze)

Na podstawie art. 17 ust. 1 / art. 17 ust. 8 / art. 17 ust. 9*) ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2024 r. poz. 184 i 1222) wnoszę o

**ZARZĄDZENIE/PRZEDŁUŻENIE*) KONTROLI OPERACYJNEJ**

w sprawie .....
(numer sprawy i jej kryptonim, oznaczenie jednostki organizacyjnej prowadzącej sprawę)

polegającej na .....
(rodzaj prowadzonej kontroli operacyjnej, o której mowa w art. 17 ust. 5 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym)

realizowanej przy wykorzystaniu:
- współpracy z podmiotem zobowiązanym*);
- oprogramowania*);
- urządzenia elektronicznego*);
- systemu informatycznego*);
- systemu teleinformatycznego*);
- innego środka .....*)
(rodzajowe wskazanie planowanego do wykorzystania środka technicznego)

przez zastosowanie jego funkcjonalności w zakresie .....,
(ogólne wskazanie funkcjonalności, która będzie wykorzystana)

zmierzającej do uzyskania materiałów w postaci .....,
(rodzajowe wskazanie danych lub informacji, których uzyskanie jest planowane)

*) Niepotrzebne skreślić.

*A template of the form containing the request from the Head of the Central Anti-Corruption Bureau (CBA) to the Regional Court in Warsaw for the authorisation or extension of surveillance. The court will be informed, for example, that the agency wishes to use software and which of its functions will be utilised.*

These changes are not enough though. Unless measures such as a privacy advocate are introduced, the proceedings remain one-sided, as there is no one to defend the right to privacy of the person being investigated.

**Furthermore, in the opinion of some judges, the second amendment was introduced in disregard of the hierarchy of legal acts and is therefore invalid.**

The Code of Criminal Procedure states that 'no reasons need be given (...) for granting a motion to which the other party has not objected, unless the ruling is subject to appeal' (Article 98(3) of the Code of Criminal Procedure). In proceedings for authorisation to conduct surveillance there is no 'other party' and a positive decision is not subject to appeal.

As the Code of Criminal Procedure is an act and takes precedence over a mere regulation – as stated by Beata Najjar, President of the Regional Court in Warsaw, the court

responsible for authorising surveillance by security services – some judges have ignored this regulation and do not provide reasons for their positive decisions.[55]

At the same time, the obligation to prepare a statement of reasons for their decisions alone does not resolve the issue of the limited time judges have at hands. As the President of the Regional Court put it, some judges use an actual 'one-size-fits-all' stamp instead of a proper statement of reasons justifying their decisions.

### 3.5.2. The draft act on oversight of security services does not solve the problem

The draft act amending certain acts 'to strengthen judicial oversight of the use of surveillance techniques'[56] is primarily intended to introduce an obligation for judges to provide reasons for their decisions regardless of whether the court has approved or rejected the application for authorisation of surveillance – a measure which had previously been unsuccessfully attempted via regulations. It also provides for the possibility of judicial oversight of surveillance that has already been authorised: the court could request access to materials gathered during the roll out of surveillance and, following their analysis, issue a ruling to suspend it.

The government states that the draft act is not intended to implement the judgment of the ECtHR:

> *The specific measures contained in the draft may address the issues identified by the European Court of Human Rights in the cited judgment in the case of Pietrzak and Bychawska-Siniarska and Others v. Poland. Nevertheless, the draft act itself does not claim to implement that judgment.*[57]

Contrary to these statements, the draft act was drawn up following informal consultations between the Ministry of Justice, the Minister Coordinator of Special Services, and representatives of the applicants concerning the enforcement of the judgment. It was there that an outline of the draft was first presented to one of the

[55] Office of the Ombudsman on YouTube, *Konferencja: Pod nadzorem/bez nadzoru. Kontrola operacyjna w państwie prawa* [Conference: Under supervision/without supervision. The use of surveillance techniques in a state governed by the rule of law], District Court Judge Beata Najjar appears at 4:37:20, https://www.youtube.com/watch?v=UW8ASvZbM6U.

[56] Draft bill act amending certain acts to strengthen judicial oversight of the use of surveillance techniques, op. cit.

[57] The report on discrepancies attached to the letter of 3 February 2026 forwarding draft act UD278 amending certain acts to strengthen judicial oversight of the use of surveillance techniques to the Standing Committee of the Council of Ministers, https://legislacja.rcl.gov.pl/projekt/12404202.

authors of this analysis. To our knowledge, no other work on the implementation of the judgment is currently underway.

The draft act requires thorough refinement though – that is if its stated objectives are not to remain merely on paper.

Firstly, the court **may** review ongoing surveillance it has authorised, but is **not required** to do so. This element of the draft act should introduce an **obligation** to review activities of security services, even if this were to apply only to limited number of cases.

Secondly, the draft does not provide for resources necessary to carry out this new task. For example more jobs, particularly in the Regional Court in Warsaw – we explained why this is important in subsection 2.2.

Thirdly, the possibility of making available to the court – at its request – materials gathered in the course of surveillance may result in the court being inundated with a volume of unprocessed material, which the court will be unable to assess in order to verify whether there is still a need to conduct the surveillance.[58] When publishing this report, the draft act was still being debated in the Polish parliament.

The argument that **the currently proposed measures are merely superficial was supported by Judge Beata Najjar**, President of the Regional Court in Warsaw, who during a conference at the Office of the Ombudsman stated as follows:

> *To be able to make a decision to terminate surveillance operation, the court would first have to assess its results, meaning it would have to examine the material gathered from the moment the surveillance was ordered until the moment of verification. (...) I cannot imagine this being feasible from an organisational point of view (...) given our current staffing capacity, the number of judges, and the workload.*[59]

[58] Panoptykon Foundation, opinion on the draft act amending certain acts to strengthen judicial oversight of the use of surveillance techniques (Sejm document 2411) of 30 April 2026, https://panoptykon.org/sites/default/files/2026-05/opinia-fundacji-panoptykon.pdf.

[59] Office of the Ombudsman on YouTube, *Konferencja: Pod nadzorem/bez nadzoru. Kontrola operacyjna w państwie prawa* [Conference: Under supervision/without supervision. The use of surveillance techniques in a state governed by the rule of law], District Court Judge Beata Najjar appears at 4:37:20, https://www.youtube.com/watch?v=UW8ASvZbM6U .

## 3.6. No one has been held accountable for the ‘Pegasus scandal’

During the 2023 election campaign, politicians emphasised the need to hold to account those responsible for using Pegasus to surveil public figures. Leaving aside the fact that these promises may have been made primarily to win the election, we believe that such accountability is necessary. Its role is, above all, to discourage the leadership and officers of security services from committing further abuses.

The Sejm Inquiry Committee and Investigation Team No. 3 at the National Prosecutor’s Office are handling the investigations. Both bodies are tasked with clarifying the scandal, although the Committee generally holds its sessions in public, whereas the Prosecutor’s Office does not.

### 3.6.1. The protracted work of the Sejm Inquiry Committee

The Sejm Inquiry Committee has been tasked with examining ‘the legality, propriety, and purposefulness of operational and reconnaissance activities undertaken, inter alia, using the Pegasus software by members of the Council of Ministers, secret services, the Police, tax inspection and customs authorities, law enforcement agencies, and the Public Prosecutor’s Office in the period from 16 November 2015 to 20 November 2023’. The Committee, chaired by MP Magdalena Sroka, began its work in 2024. To date, it has held 129 meetings, 77 of which were substantive in nature (i.e. a witness was heard or an expert opinion was obtained).

The Committee dealt with both examining the adequacy of surveillance conducted with the use of spyware and assessing the legality and appropriateness of the purchase of the Pegasus software. It sought to clarify the circumstances surrounding the use of the Pegasus system and determine the number of interventions it was used for. It also investigated the issue of potential espionage and sought to establish whether there had been an illegal disclosure of information concerning the interests of the Polish secret services to foreign intelligence services through the improper, illegal, or inappropriate use of the Pegasus or another software.

Despite the controversy surrounding the Committee's legal status[60] and the resulting difficulties in securing the attendance of certain witnesses,[61] **the Committee ultimately heard 79 people, 22 of whom were granted anonymity**. 64 of the 129 sessions were held either fully or partially out of camera so that the witnesses being questioned could provide Members of Parliament with information of a confidential nature.

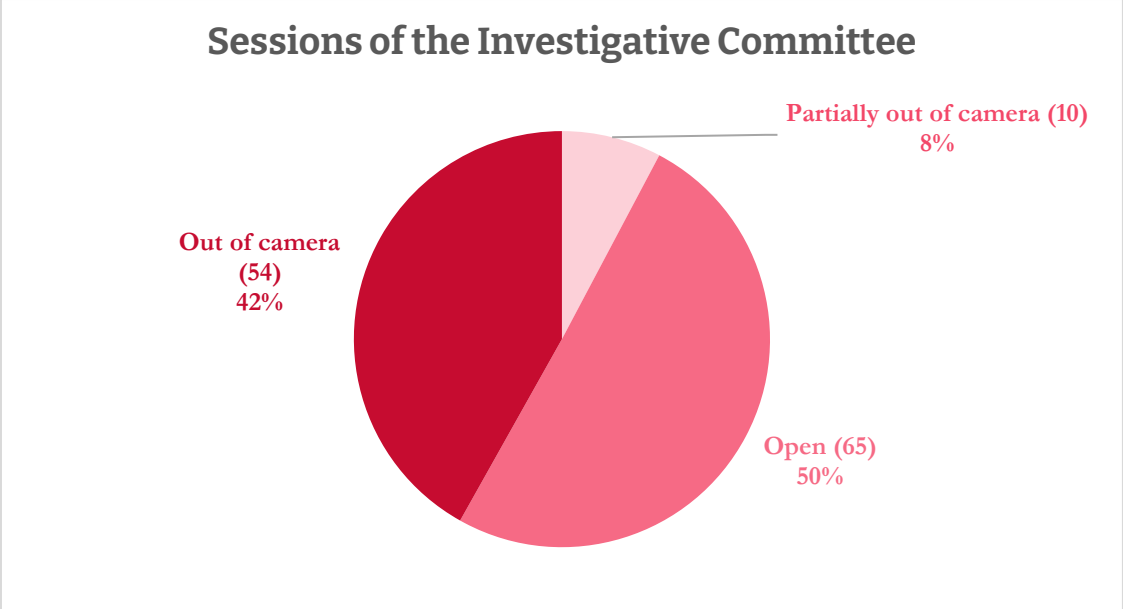



*Figure 2. Own compilation based on information from the Sejm website: https://sejm.gov.pl/Sejm10.nsf/PosKomZrealizowane.xsp?komisja=SKPG.*

At the time of writing this report, the Committee has not yet published its final findings. According to official sources, their final report will be divided into public, classified, and top-secret sections. The public will only be able to access the public section of the report.

[60] The District Public Prosecutor's Office in Warsaw, *Sejmowa Komisja Śledcza ds. Pegasusa legalna. Odmowa wszczęcia śledztwa z uwagi na brak znamion czynu zabronionego* [The Sejm Inquiry Committee on Pegasus is lawful. Refusal to open an investigation due to the absence of evidence of a criminal offence], https://www.gov.pl/web/po-warszawa/sejmowa-komisja-sledcza-ds-pegasusa-legalna-odmowa-wszczecia-sledztwa-z-uwagi-na-brak-znamion-czynu-zabronionego.

[61] PAP, *Były szef CBA nie stawił się na komisji ds. Pegasusa. Będzie wniosek o karę i doprowadzenie* [The former head of the CBA failed to appear before the Pegasus committee. A motion will be tabled for disciplinary action and for him to be brought before the committee], https://www.pap.pl/aktualnosci/byly-szef-cba-nie-stawil-sie-na-komisji-ds-pegasusa-bedzie-wniosek-o-kare-i.

The report was due to be published in April 2026. The delay in its publication is reportedly due to the large volume of classified material.[62]

### 3.6.2. The National Prosecutor's Office Investigation Team has not brought any charges

The National Prosecutor's Office Investigation Team has been conducting an investigation since March 2024.[63] Its task is to examine the legality, legitimacy, and propriety of the use of Pegasus by public officials. The prosecution team was also to examine a report of a suspected offence, which was filed as a result of the work of the Senate Special Committee (see Part 2 of the committee's report).

The investigation conducted by the National Prosecutor's Office covers three types of cases:

1) Abuse of power or dereliction of duty by public officials, i.e. the unlawful use of the Pegasus software as a means of conducting surveillance, as well as the unlawful use of materials obtained as a result thereof,

2) Incitement or aiding and abetting the unjustified use of Pegasus,

3) Misleading other authorities in order to use the Pegasus software in specific cases.

To date charges have been brought for abuse of power, involving, among other things, the 'deceptive' misleading of the court 'as to the existence of grounds for the application and extension of surveillance', or dereliction of duty in connection with failing to obtain the required accreditation for the use of Pegasus. These charges were brought against former heads, a deputy-head, and two officers of three intelligence agencies.

No one has yet been formally charged.

***

In summary, the changes made so far amount to regulations that expand the scope of information on the basis of which a court authorises surveillance or denies it. But

---

[62] TVP Info, *Komisja Pegasusa kończy prace. Raport podzielony na część jawną i tajną* [The Pegasus Committee is completing its work. The report is divided into a public and a confidential section], https://www.tvp.info/92515418/sejmowa-komisja-ds-pegasusa-ujawni-czesc-raportu-czesc-pozostanie-tajna.

[63] National Public Prosecutor's Office, *Komunikat o zespole śledczym ds. Pegasusa*, [Statement on the Pegasus investigation team], https://www.gov.pl/web/prokuratura-krajowa/komunikat-o-zespole-sledczym-ds-pegasusa.

regulations requiring the court to justify its decisions are ineffective, work on the Code of Operational Procedure has been abandoned, and the judgments of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) are being implemented to a very limited extent.

Only the personnel has changed. After 2023, new people took the leadership of all secret services. Their former heads and those involved in the Pegasus scandal have still not been held accountable though. Politicians have failed to deliver on their promises to introduce oversight of security services' activities. This also means that the legal framework governing the use of spyware has not been fixed. In the next section, we outline what needs to change.

# 4. Recommendations for a legal framework for spyware

**In this chapter, we:**

- Explain why security services wish to use spyware,
- Present a list of necessary changes to Polish law regarding spyware and – more broadly – surveillance techniques.

## 4.1. Why security services should be allowed to use spyware legally

**The key argument in favour of Pegasus being permissible under Polish law comes down to the assertion that security services need it to operate effectively**. This argument is put forward primarily by Law and Justice (PiS) politicians and those responsible for leading the secret services during the PiS government. As former heads of Polish services argue in their appeal to the government:

> *Providing the security services with the technology necessary for the effective performance of their tasks is not only a duty, but indeed an obligation of the Heads of Special Services.*[64]

[64] Stanisław Żaryn's profile on X, https://x.com/StZaryn/status/2028417655468650894?s=20.

According to the recommendations of the high-level working group on data access for effective law enforcement, as early as 2019 over 22% of messages were sent via *end-to-end* encrypted messaging apps, making them inaccessible to law enforcement agencies. The share of such messaging apps in everyday communication is rising sharply. Currently, around 90% of communication takes place via messaging apps – including those that encrypt communication by default.[65]

It is precisely the growing popularity of encrypted communication that is the most frequently cited argument in favour of the use of spyware by the authorities.[66]

The European Commission has already announced, in its European Internal Security Strategy 'ProtectEU', that it intends 'to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and fundamental rights'.[67]

The Polish government has also announced plans to develop a system 'enabling the effective recording of content generated by individuals involved in terrorist activities using instant messaging services' and to precisely regulate the rules for the use of 'offensive cyber tools against contemporary communication tools, including interpersonal communication'. This is to be accompanied by the development of technical capabilities in this area.[68]

We are convinced that the Polish security services already possess the technological tools that enable them to access *end-to-end* encrypted communications. Such capabilities are provided by spyware.

**At the same time, the Polish legal system provides no basis for the use of such software. Despite much fanfare, authorities have not introduced legal changes allowing its use, and the system of judicial oversight of surveillance remains highly flawed. This means that Polish security services operate in an unclear legal environment, and citizens are not protected against abuses.**

---

[65] Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en.

[66] The difficulty in countering this argument lies in the fact that the alternative – weakening communication encryption (as proposed, for example, in the context of Child Sexual Abuse Regulation) – is far more dangerous, as it affects everyone.

[67] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148.

[68] Resolution No. 92 of the Council of Ministers of 10 March 2026 on the Cybersecurity Strategy of the Republic of Poland, https://monitorpolski.gov.pl/M2026000030901.pdf.

If security services are to carry out their tasks effectively without breaching the law, the following are needed:

1) Systemic changes to the oversight of the use of surveillance techniques by services,
2) A precise legal framework for the use of spyware.

In our view, **spyware should be a specific, distinct form of covert interference with citizens' privacy**. We therefore propose two levels of change:

1) In the general principles governing the use of surveillance techniques, which should apply to both traditional wiretapping and spyware (see 4.2),
2) The regulation of **spyware specifically** (see 4.3).

## 4.2. Changes to the use of surveillance techniques

### 4.2.1. Effective prior judicial review

**The model for obtaining court authorisation to use surveillance techniques requires the following changes:**

1) The judge should be able to examine all the case material, not just the part that justifies the need for surveillance;
2) The judge should be provided with adequate resources, i.e. time, technical and administrative support, and technical expertise to examine each case thoroughly;
3) The proceedings should be balanced by the presence of a privacy advocate defending the rights of the person concerned, who should have the opportunity to appeal against the court's decision authorising surveillance;
4) A request to the court to authorise surveillance should clearly specify the objectives, scope, and methods, including information on which techniques are to be used, what data will be obtained, and whether historical data will be obtained.

### 4.2.2. Obligation to notify the subject about surveillance and the right to appeal

It is also of fundamental importance to **grant the individual:**

1) The right to be informed that they have been the subject of interest of secret surveillance measures,
2) The right to access to their personal data, in line with data protection law.

The obligation to notify individuals who have been subject to surveillance should, as a rule, be fulfilled 12 months after the end of the operation. Of course, exceptions to this rule are possible, for example on grounds of national security (provided that court approval is obtained).

Such notification should be followed by a possibility of appealing against the court's decision.

### 4.2.3. Ex-post oversight by a specialised body or court

Furthermore, it is essential to introduce **a mechanism for the effective verification of activities of the security services while they are conducting surveillance**.

In our view, the optimal solution would be to establish a specialised oversight body – as we recommended solution in our report *Saddling Pegasus: Respect for Civil Rights in the Activities of the Secret Services – Reform Principles.*[69]

Only the combined introduction of these three changes will strengthen oversight of the security services' activities.

## 4.3. Specific regulations concerning spyware

We also call for the adoption of safeguards specifically concerning spyware. **Regulations should:**

1) **Distinguish between the passive and active functions of such software** (see section 1.1.) and prohibit the use of the latter,
2) **Permit the use of spyware only in cases of particular gravity**, e.g. those related to terrorism. In any case, the list of acceptable applications should be exhaustive and limited to most serious crimes,
3) **Guarantee the security of data obtained via spyware so as to prevent access by untrusted providers**. Perhaps the solution in this area lies in the notion to create a local technology for accessing the content stored on the phones of individuals involved in terrorist or espionage activities, which was outlined in the Cybersecurity Strategy of the Republic of Poland.[70]

[69] Panoptykon Foundation, *Osiodłać Pegaza. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy* [Saddling Pegasus: Upholding civil liberties in the activities of the secret services – the principles of the reform], https://panoptykon.org/sites/default/files/osiodlac_pegaza_-_jak_powinien_wygladac_nadzor_nad_sluzbami._raport_ekspertow.pdf.

[70] Resolution No. 92 of the Council of Ministers of 10 March 2026 on the Cybersecurity Strategy of the Republic of Poland, https://monitorpolski.gov.pl/M2026000030901.pdf.

# Closing remarks

The above recommendations cover the most important changes necessary to legalise the use of spyware and to ensure that oversight of the use of surveillance techniques in Poland strikes an appropriate balance between the need to ensure the effectiveness of the security services' operations and the minimisation of the risk of abuse. We regard them as a starting point for the necessary discussion.

Detailed proposals for changes can be found, inter alia, in the Ombudsman's report *Implementation of the judgment of the European Court of Human Rights in the case of Pietrzak and Bychawska-Siniarska and others v. Poland (case nos. 72038/17 and 25237/18). The report on necessary changes to the regulations governing the pre-trial and trial monitoring, and recording of conversations*[71] and in the report *Saddling Pegasus*. Another important point of reference is the draft Code of Operational Procedure, which addresses many of the challenges described above.

Our recommendations do not, however, cover other issues requiring resolution within the scope of the security services' operations, such as the question of access to telecommunications data. In this regard, we refer to the report by the Ombudsman.[72]

As the recommendations are addressed to the Polish legislature, we do not address here issues whose resolution lies within the remit of the European Union, and which are described in detail in the report of the PEGA investigative committee and in the aforementioned EDRi.

---

[71] Office of the Ombudsman, *Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprocesową oraz procesową kontrolę i utrwalanie rozmów* [Implementation of the judgment of the European Court of Human Rights in the case of Pietrzak and Bychawska-Siniarska and Others v. Poland (cases nos. 72038/17 and 25237/18). Report on the necessary amendments to the provisions governing the extrajudicial and judicial monitoring and recording of conversations], https://bip.brpo.gov.pl/sites/default/files/2025-11/Raport_wykonanie_wyroku_etpc_inwigilacja_3_07_2025.pdf.

[72] Office of the Ombudsman, *Opinia RPO ws. pozyskiwania danych telekomunikacyjnych obywateli przez służby specjalne i policję. Odpowiedź MC* [Opinion of the Ombudsman on the collection of citizens' telecommunications data by the secret services and the police. Response from the Ministry of Digital Affairs], https://bip.brpo.gov.pl/pl/content/rpo-retencja-danych-policja-sluzby-koordynator-mswia-ms-mc.

# Sources


1. EDRi, *Spyware and state abuse. The case for an EU-wide ban*, https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/.

2. Share Foundation, *A privacy nightmare: understanding spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

3. Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.

4. Citizen Lab, *HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

5. Information on the total number of individuals against whom a request was made for the interception and recording of communications or for the authorisation of surveillance in 2023, https://orka.sejm.gov.pl/Druki10ka.nsf/0/7522A4519FE790ACC1258B01003A2A38/%24File/308.pdf.

6. The Guardian, *Poland launches inquiry into previous government's spyware use*, https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use.

7. Report of the Special Committee on the Investigation of Cases of Illegal Surveillance, Their Impact on the Electoral Process in the Republic of Poland, and the Reform of the Special Services, https://www.senat.gov.pl/download/gfx/senat/pl/defaultaktualnosci/1924/15764/1/raport_koncowy_z_prac_komisji_nadzwyczajnej.pdf.

8. Bankier.pl, *Hermeliński: Wybory w 2019 roku, choć nie były sfałszowane, nie były uczciwe* [The 2019 elections, while not rigged, were not fair], https://www.bankier.pl/wiadomosc/Hermelinski-Wybory-w-2019-roku-choc-nie-byly-sfalszowane-nie-byly-uczciwe-8266533.html.

9. Rzeczpospolita, *Adam Bodnar: Zbigniew Ziobro powinien trafić do aresztu. Zachodzi obawa mataczenia lub ucieczki* [Zbigniew Ziobro should be taken into custody. There is a risk that he might tamper with evidence or abscond], https://www.rp.pl/polityka/art43290211-adam-bodnar-zbigniew-ziobro-powinien-trafic-do-aresztu-zachodzi-obawa-mataczenia-lub-ucieczki.

10. The Guardian, *Second Italian journalist allegedly targeted with 'mercenary spyware'*, https://www.theguardian.com/world/2025/may/01/second-italian-journalist-allegedly-targeted-with-mercenary-spyware.

11. Citizen Lab, *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*, https://citizenlab.ca/research/a-first-look-at-paragons-proliferating-spyware-operations/#h-3-whatsapps-paragon-investigation.

12. Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

13. Citizen Lab, *Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles*, https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

14. Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

15. Access Now, *Spyware in Serbia: civil society under attack*, https://www.accessnow.org/spyware-attack-in-serbia/.

16. Amnesty International, *Serbia: 'A Digital Prison': Surveillance and the suppression of civil society in Serbia*, https://www.amnesty.org/en/documents/eur70/8813/2024/en/.

17. International Consortium of Investigative Journalists, *Greek court convicts Intellexa founder Tal Dilian, three others in wiretapping scandal*, https://www.icij.org/investigations/cyprus-confidential/greek-court-convicts-intellexa-founder-tal-dilian-three-others-in-wiretapping-scandal/.

18. Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

19. The Record, *Intellexa founder, three others sentenced to 8 years in prison over Greek spyware scandal*, https://therecord.media/spyware-intellexa-greece-sentenced.

20. Ekathimerini.com, *Four businesspeople found guilty in 2022 spyware scandal*, https://www.ekathimerini.com/news/1296353/four-businesspeople-found-guilty-in-spyware-trial/.

21. Citizen Lab, *Saudi Arabia Ordered to Pay £3m to London Dissident Over Pegasus Spying*, https://citizenlab.ca/saudi-arabia-ordered-to-pay-3m-to-london-dissident-over-pegasus-spying/.

22. Judgment in the case of Ghanem Al-Masarir v. the Kingdom of Saudi Arabia, https://caselaw.nationalarchives.gov.uk/ewhc/kb/2026/119.

23. The Guardian, *Saudi dissident awarded £3m damages threatens enforcement action if he is not paid*, https://www.theguardian.com/world/2026/jan/30/saudi-dissident-awarded-3m-damages-threatens-enforcement-action-if-he-is-not-paid.

24. Share Foundation, *A Privacy Nightmare: Understanding Spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

25. Resolution of the Supreme Court of 26 April 2023, ref. no. I ZI 50/22, https://www.sn.pl/sites/orzecznictwo/orzeczenia3/i%20zi%2050-22.pdf.

26. Judgment of 11 May 2023, ref. no. II AKa 480/21, https://www.saos.org.pl/judgments/501168.

27. The Sejm Inquiry Committee to examine the legality, propriety, and appropriateness of operational and intelligence activities undertaken, inter alia, using Pegasus software by members of the Council of Ministers, the secret services, the Police, tax inspection and customs authorities, law enforcement agencies and the Public Prosecutor's Office during the period from 16 November 2015 to 20 November 2023 (SKPG), https://sejm.gov.pl/Sejm10.nsf/agent.xsp?symbol=KOMISJASL&NrKadencji=10&KodKom=SKPG.

28. Rzeczpospolita, *Sędzia Igor Tuleya: Możliwe, że zgodziłem się na Pegasusa* [Judge Igor Tuleya: It is likely that I authorised the use of Pegasus], https://www.rp.pl/sady-i-trybunaly/art39874451-sedzia-igor-tuleya-mozliwe-ze-zgodzilem-sie-na-pegasusa.

29. Prawo.pl, *Kontrola operacyjna wymknęła się... spod kontroli* [Surveillance got... out of control], https://www.prawo.pl/prawnicy-sady/sedziowie-nie-moga-byc-manipulowani-przez-sluzby,525859.html.

30. Office of the Ombudsman, *Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprocesową oraz procesową kontrolę i utrwalanie rozmów* [Implementation of the judgment of the European Court of Human Rights in the case of Pietrzak and Bychawska-Siniarska and Others v. Poland (cases nos. 72038/17 and 25237/18). Report on the necessary amendments to the provisions governing the extrajudicial and judicial monitoring and recording of conversations], https://bip.brpo.gov.pl/sites/default/files/2025-11/Raport_wykonanie_wyroku_etpc_inwigilacja_3_07_2025.pdf.

31. Colonel Przemysław Leśniak's profile on X, https://x.com/przemkolesniak/status/2029262770776977767.

32. The National Public Prosecutor's Office, *ABW: system Pegasus powinien podlegać akredytacji bezpieczeństwa teleinformatycznego* [ABW: the Pegasus system should be subject to ICT security accreditation], https://www.gov.pl/web/prokuratura-krajowa/abw-system-pegasus-powinien-podlegac-akredytacji-bezpieczenstwa-teleinformatycznego.

33. Spider's Web, *Pegasus jest jeszcze bardziej nielegalny, niż się wydawało* [Pegasus is even more illegal than previously thought], https://spidersweb.pl/2025/05/pegasus-nie-mial-akredytacji-bezpieczenstwa.html.

34. Zaufana Trzecia Strona, *5 powodów, dla których używanie Pegasusa w Polsce nie mogło być legalne* [5 reasons why using Pegasus in Poland could not have been legal],

https://zaufanatrzeciastrona.pl/post/5-powodow-dla-ktorych-uzywanie-pegasusa-w-polsce-nie-moglo-byc-legalne/.

35. European Parliament recommendation of 15 June 2023 to the Council and the Commission following an inquiry into allegations of breaches of Union law and maladministration in its application in relation to Pegasus and equivalent spyware (2023/2500(RSP)), paragraph 32, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:C_202400494.

36. Donald Tusk – official YouTube channel, *Donald Tusk: Kongres 100 konkretów, Tarnów, 9.09.2023* [Donald Tusk: The '100 Specifics' Congress, Tarnów, 9 September 2023], https://www.youtube.com/live/rLzOWVm3epo?t=3720s.

37. Radosław Sikorski's profile on X, *https://x.com/sikorskiradek/status/1712440684542599541*.

38. Coalition Agreement of 10 November 2023, https://platforma.org/upload/document/203/attachments/433/UmowaKoalicyjna.pdf.

39. Draft Act on the Code of Operational Procedure of 17 April 2023, https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf.

40. Panoptykon Foundation, *Inwigilacja w Polsce narusza twoje prawa. Ważny wyrok Europejskiego Trybunału Praw Człowieka* [European Court of Human Rights: secret surveillance in Poland violates citizens' privacy rights], https://en.panoptykon.org/ECHR-surveillance-judgment-Poland-2024.

41. Ministry of the Interior and Administration, *Konferencja prasowa dotycząca orzeczenia ETPC ws. kontroli operacyjnej w Polsce* [Press conference on the ECtHR ruling regarding the use of surveillance techniques in Poland], https://www.gov.pl/web/mswia/konferencja-prasowa-dotyczaca-orzeczenia-etpc-ws-kontroli-operacyjnej-w-polsce.

42. Panoptykon Foundation, *Wzmocniona kontrola nad działaniami Krajowej Administracji Skarbowej – projekt opublikowany po apelu organizacji* [Tighter oversight of the National Revenue Administration's activities – draft regulation published following an appeal by the organisation], https://panoptykon.org/krajowa-administracja-skarbowa-po-apelu.

43. Draft act amending certain acts to strengthen judicial oversight of the use of surveillance techniques, https://sejm.gov.pl/Sejm10.nsf/druk.xsp?documentId=63F5DE808433ECBCC1258DD90031980F.

44. Office of the Ombudsman on YouTube, *Konferencja: Pod nadzorem/bez nadzoru. Kontrola operacyjna w państwie prawa* [Conference: Under supervision/without supervision. The use of surveillance techniques in a state governed by the rule of law], https://www.youtube.com/watch?v=UW8ASvZbM6U.

45. The report on discrepancies attached to the letter of 3 February 2026 forwarding draft act UD278 amending certain acts to strengthen judicial oversight of the use of surveillance

techniques to the Standing Committee of the Council of Ministers, https://legislacja.rcl.gov.pl/projekt/12404202.

46. Panoptykon Foundation, opinion on the draft act amending certain acts to strengthen judicial oversight of the use of surveillance techniques (Sejm document 2411) of 30 April 2026, https://panoptykon.org/sites/default/files/2026-05/opinia-fundacji-panoptykon.pdf.

47. The District Public Prosecutor's Office in Warsaw, *Sejmowa Komisja Śledcza ds. Pegasusa legalna. Odmowa wszczęcia śledztwa z uwagi na brak znamion czynu zabronionego* [The Sejm Inquiry Committee on Pegasus is lawful. Refusal to open an investigation due to the absence of evidence of a criminal offence], https://www.gov.pl/web/po-warszawa/sejmowa-komisja-sledcza-ds-pegasusa-legalna-odmowa-wszczecia-sledztwa-z-uwagi-na-brak-znamion-czynu-zabronionego.

48. PAP, *Były szef CBA nie stawił się na komisji ds. Pegasusa. Będzie wniosek o karę i doprowadzenie* [The former head of the CBA failed to appear before the Pegasus committee. A motion will be tabled for disciplinary action and for him to be brought before the committee], https://www.pap.pl/aktualnosci/byly-szef-cba-nie-stawil-sie-na-komisji-ds-pegasusa-bedzie-wniosek-o-kare-i.

49. TVP Info, *Komisja Pegasusa kończy prace. Raport podzielony na część jawną i tajną* [The Pegasus Committee is completing its work. The report is divided into a public and a confidential section], https://www.tvp.info/92515418/sejmowa-komisja-ds-pegasusa-ujawni-czesc-raportu-czesc-pozostanie-tajna.

50. The National Public Prosecutor's Office, *Komunikat o zespole śledczym ds. Pegasusa* [Statement on the Pegasus investigation team], https://www.gov.pl/web/prokuratura-krajowa/komunikat-o-zespole-sledczym-ds-pegasusa.

51. Stanisław Żaryn's profile on X, https://x.com/StZaryn/status/2028417655468650894?s=20.

52. Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en.

53. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148.

54. Resolution No. 92 of the Council of Ministers of 10 March 2026 on the Cybersecurity Strategy of the Republic of Poland, https://monitorpolski.gov.pl/M2026000030901.pdf.

55. Panoptykon Foundation, *Osiodłać Pegaza. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy* [Saddling Pegasus: Upholding civil liberties in the activities of the secret services – the principles of the reform], https://panoptykon.org/sites/default/files/osiodlac_pegaza_-_jak_powinien_wygladac_nadzor_nad_sluzbami._raport_ekspertow.pdf.

56. Office of the Ombudsman, *Opinia RPO ws. pozyskiwania danych telekomunikacyjnych obywateli przez służby specjalne i policję. Odpowiedź MC* [Opinion of the Ombudsman on the collection of citizens' telecommunications data by the secret services and the police. Response from the Ministry of Digital Affairs], https://bip.brpo.gov.pl/pl/content/rpo-retencja-danych-policja-sluzby-koordynator-mswia-ms-mc.

# About the Panoptykon Foundation

At the Panoptykon Foundation, we have been campaigning for laws that protect freedom and privacy since 2009. We keep an eye on the state and tech corporations, expose the abuse of power, and empower people to live consciously in the digital world.

We work to ensure that new technologies serve society and that people have control over how their data is used.

For over 17 years, we have been fighting for oversight of the activities of the security services. In 2010, we revealed statistics on the Polish security services' acquisition of phone call records and other telecommunications data. In 2024, our efforts led to a ruling by the European Court of Human Rights stating that Polish regulations on surveillance require systemic changes. We have worked with the European Parliament's PEGA Committee and the Polish Senate Special Committee investigating cases of Pegasus being used to surveil citizens. We are also a part of the European PEGA Coalition, which aims to litigate and publicly denounce the unacceptable and disproportionate use of spyware in Europe, especially when deployed by intelligence and law enforcement agencies.

Join the fight for freedom and privacy! Support our work with a donation: https://en.panoptykon.org/donate

***

Compiled by: Wojciech Klicki, Anna Obem, Zuzanna Rżysko

Translation: Maria Zawadzka

Consultation: Lori Roussey

Cover: Paweł Smardzewski

Panoptykon Foundation

Panoptykon.org

August 2026



PANOPTYKON FOUNDATION