European Parliament

Setting spyware standards after the Pegasus scandal

SUMMARY

In June 2023, following its investigation into Europe's spyware scandal, the European Parliament issued a final recommendation identifying country-specific shortcomings and proposing EU standards for the use of spyware.

In line with EU competences, Parliament proposes a narrow focus for its spyware surveillance standards, limiting them to law enforcement activities. Among these spyware surveillance standards, Parliament proposed a range of safeguards, including prior judicial approval, necessity and proportionality requirements, strong and independent post-surveillance oversight, the duty to notify targeted persons and other persons concerned, access to redress and meaningful remedies, and data deletion requirements.

Member States embroiled in the spyware scandal are making progress – albeit uneven – towards meeting these standards. Greece has amended its intelligence law in the wake of the spyware scandal, but it remains to be seen whether it will address outstanding shortcomings. Spain has announced further efforts to strengthen its legal framework, although Parliament considered the country's legal framework fundamentally compliant. Rule of law concerns persist in Hungary. Poland is investigating the alleged spyware abuses thoroughly, and is making decisive efforts to improve its legal framework.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Hendrik Mildebrath
Members' Research Service

PE 766.262 – November 2024

Introduction

In 2021, media organisations broke the story that various EU and non-EU governments had used the commercial spyware 'Pegasus' against Members of the European Parliament (MEPs), journalists, politicians, diplomats, law enforcement officials, lawyers, business people and civil society actors, for political and even criminal purposes. Pegasus was designed to breach mobile phones and extract vast amounts of data processed by the target system, including text messages, call interceptions, passwords, locations, microphone and camera recordings, and information from installed apps. While other institutions shied away from taking meaningful action, the European Parliament spearheaded public efforts to investigate and curb spyware abuse. In response to what quickly became known as 'Europe's Watergate', Parliament set up the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA committee). In March 2023, PEGA adopted a 145-page report on the results of its investigation; and Parliament adopted its final recommendation in June 2023. Although the PEGA committee ceased to exist when its extended mandate expired on 9 June 2023, the former rapporteur announced that Parliament would

> *continue to monitor, to pierce, to ask questions, to dig, to put pressure on the governments, to give support to those journalists, lawyers, independent bodies, anybody who is investigating and bringing to light the practices of our governments.*

Meanwhile, legislative reforms and the development of standards for the use of spyware are picking up momentum. The EU co-legislators adopted the European Media Freedom Act (EMFA), which contains a provision that explicitly protects devices and tools used by media service providers, their editorial staff and related persons against the deployment of intrusive surveillance software such as spyware by Member States (Article 4(3)-(7)). The Council of Europe has requested a report on a rule of law and human rights-compliant regulation of spyware, expected to be adopted in December 2024. Reportedly, the European Commission is also working on 'minimum safeguards and conditions' that should be implemented 'irrespective of the purpose of the surveillance'.[1]

Parliament set out its own spyware standards in paragraph 32 of its final recommendation. The Member States embroiled in the spyware scandal are making uneven progress meeting these standards.[2] The European Commission draws a similar conclusion in its 2024 Rule of Law Report.

European Parliament spyware recommendation

In its final recommendation, Parliament found that both EU Member States and non-EU countries had used Pegasus and similar spyware for political and even criminal purposes. Parliament was concerned that some Member States had spied on targets under the false pretence of 'national security', to escape EU oversight. It concluded that Greek and, in particular, Polish and Hungarian legal frameworks and practices violated EU law, and did not offer citizens sufficient protection. It found that Spain's regulatory framework is fundamentally compliant, but that some reforms are necessary, while Cyprus's application of EU export controls exhibited evidence of maladministration.

To improve the situation, Parliament drew up country-specific recommendations for these Member States. Additionally, it envisaged stronger institutional and legal safeguards to ensure fundamental rights-compliant use of spyware by law enforcement. It developed strict **spyware surveillance standards** that include conditions for ordering, authorising, executing, and overseeing spyware operations, along with requirements for effective redress. Parliament acknowledges that surveillance operations for **national security** purposes in principle remains the exclusive competence of Member States, but points out that EU law regulates certain national security surveillance activities indirectly. Given concerns over the unjustified invocation of national security, Parliament considers that a clear definition of the term is necessary. Surveillance in the name of national security should be the exception rather than the rule in a democratic transparent society.

Additionally, Parliament proposes to limit the **circulation of commercial spyware** on the EU market to spyware designed in line with its envisaged spyware standards ('rule of law by design'). While

Parliament suggests permitting the sales of functionally compliant spyware technologies, it recommends prohibiting 'hacking as a service', including technical, operational and methodological support.

Parliament called on the **Commission** to monitor the implementation of its recommendations, to enforce existing EU laws more stringently, and to follow up on possible abuses and other rule of law deficiencies. It also tasked the Commission with drafting new laws as proposed by Parliament, notably regulating EU spyware surveillance standards and the placing of spyware on the market.

EU competences for setting spyware surveillance standards

Recognising that EU law can, at best, regulate the use of spyware for national security purposes indirectly,[3] Parliament recommends regulating the use of spyware for law enforcement based on the Treaty provisions relating to judicial cooperation in criminal matters (Chapter 4 of Title 5 of the Treaty on the Functioning of the European Union, TFEU).[4] Under this approach, qualified surveillance operations and frameworks would become subject to EU spyware standards, while national security operations would, at best, be regulated indirectly by EU data protection and privacy rules, and – in most cases – remain entirely outside the scope of application of EU law.

The question arises of whether such standards would cover cases in which Member States repeatedly apply lenient national security provisions to those activities of law enforcement surveillance that do not qualify as matters of national security within the meaning of EU law. Although the EU concept of national security (still defined only rudimentarily) may generously accommodate different national understandings of this concept, it would hardly include abusive activities aimed at targeting political opponents or minorities. This would amount to a carte blanche for arbitrary or even anti-democratic surveillance activities. Arguably, the Court of Justice of the European Union (CJEU) can at least conduct a limited abuse control as regards the repeated and evident misapplication of lenient national security provisions to justify data processing for other purposes. Thus, arguably, where authorities frequently rely on national security provisions to surveil opposition figures or journalists, the application of these provisions, and possibly the intelligence operations themselves, would remain subject to EU law and oversight.

However, even with explicit spyware surveillance standards, the aggrieved parties would face challenges obtaining remedies under EU law. Essentially, they do not themselves qualify as applicants, and cannot challenge Member State authorities before the CJEU. Instead, they would need to rely on the European Commission to launch infringement proceedings, or on national courts to file preliminary references with the CJEU.

In addition, aggrieved parties may invoke the violation of their human rights and seek redress before the European Court of Human Rights (ECtHR). EU spyware standards would not apply, but might serve as an interpretive tool for the ECtHR. Additionally, as mentioned earlier, the Council of Europe has requested a report on a rule of law and human rights-compliant regulation of spyware (expected in December 2024), which may likewise serve as an interpretive tool in the future.

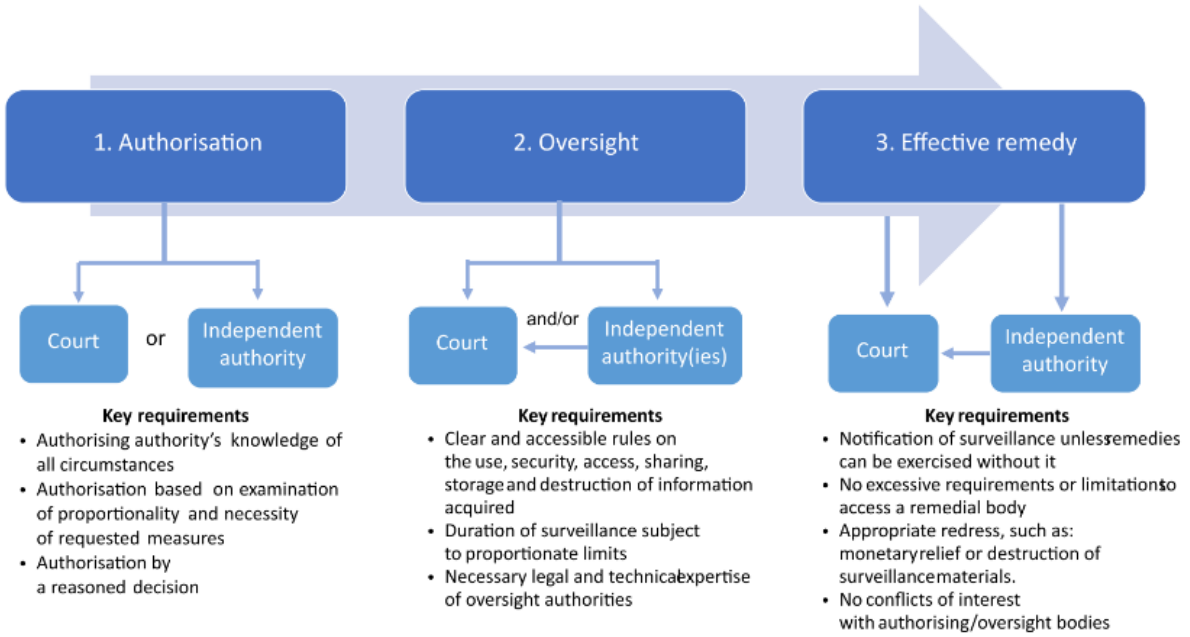
Former United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, testified before the PEGA committee that the use of spyware equivalent to Pegasus would fail to meet the requirements under the international human rights to privacy and to freedom of opinion and expression.[5] So far, cases against Greece, Hungary and Poland have reached the ECtHR, but only the Greek *Koukakis* case ended in a dismissal for a breach of confidence.

While the ECtHR recognises that Member States have 'a margin of appreciation in determining what objectives contribute to national security and what means are best suited to achieving such objectives', it can examine the limits of this discretion.[6]

Parliament's spyware surveillance standards

At the PEGA committee's request, the EU Agency for Fundamental Rights (FRA) updated its study on Surveillance by intelligence services. It derived key requirements for surveillance operations from ECtHR and CJEU case law, developing a framework for understanding spyware standards.

Figure 1 – Oversight and review of surveillance: Main requirements according to ECtHR and CJEU case law



Source: FRA, Surveillance by intelligence services, 24 May 2023.

Drawing on CJEU and ECtHR case law and reports by the Venice Commission and FRA, Parliament devised a set of strict spyware surveillance standards for law enforcement in its final recommendation of June 2023. Most notably, it recommends:

> **(a)** and **(c)** requiring prior judicial authorisation for spyware surveillance and limiting such authorisation to necessary and proportionate measures aimed at investigating a specific, closed list of serious crimes that pose a genuine threat to national security;[7]
> **(b)** restricting the targeting to individual devices or accounts, not internet and technology service providers, and making extensions conditional on further judicial authorisation;
> **(d)** making access to privileged data conditional on establishing sufficient grounds under judicial oversight and based on a common framework;
> **(e)** adopting specific rules for surveillance with spyware accounting for specific risks;[8]
> **(h)** and **(i)** respecting the right of notification by ensuring that authorities disclose a set of specific details to the targeted persons and other persons concerned after the surveillance operation has ended;
> **(j)** and **(k)** ensuring effective and independent post-surveillance oversight as well as a central role for judicial surveillance (*ex ante* or *ex post*);
> **(l)** and (m) ensuring access to redress and meaningful remedies for direct and indirect targets and those claiming to be adversely affected;
> **(n)** improving free access to technological expertise for those targeted;
> **(o)** allowing those accused of crimes to review evidence, and rejecting any blanket application of national defence secrecy rules;
> **(p)** mandating deletion of irrelevant data, and of all data after the investigation has ended;
> **(r)** adopting admissibility of evidence standards accounting for the risk of false or manipulated information;

(s) obliging Member States to notify each other when surveiling citizens or residents of another Member State or of a mobile number of a carrier in another Member State;
(t) including a marker in spyware software so oversight bodies can identify the deploying authority in the event of suspicion of abuse.

The European Parliament's standards exceed the minimum human rights standards established to date by the ECtHR and the CJEU in their interpretations of the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights.

State of play of national implementation

Member States have adopted many different laws that empower authorities to use secret surveillance, such as police acts, criminal procedural laws, and intelligence laws. However, they primarily invoked intelligence laws as the basis of their spyware surveillance operations. The question arises of how the applicable national laws would measure up to Parliament's envisaged spyware standards, and whether the Member States embroiled in the spyware scandal have made progress in implementing the spyware standards.[9]

Assessing these intelligence laws against the envisaged spyware standards bears particular challenges: firstly, their application to individual spyware scenarios is uncertain, given ambiguities around case-specific facts and legal interpretations. Although intelligence laws are strongly linked to national security interests, some of them simultaneously regulate law enforcement surveillance activities (e.g. in Greece and Hungary). Secondly, some intelligence laws may not be formally objectionable, but misapplied systematically by authorities. For instance, authorities may systematically apply lenient national security provisions instead of law enforcement provisions, while the cases do not meet the EU criteria for national security. Thirdly, the scope of the envisaged EU spyware standards for law enforcement is not yet determined, and it is therefore not clear what surveillance operations and regulations would be covered. For instance, the Law Enforcement Directive (EU) 2016/680 (LED) exempts 'activities of agencies or units dealing with national security issues' (recital 14 LED), which can be interpreted in different ways. It is worth noting that, surveillance activities do not automatically qualify as law enforcement activities within the meaning of EU law, where they do not meet the national security threshold. They must qualify as law enforcement activities and meet other (still indeterminate) scope requirements.

Ultimately, many intelligence laws – whether statutorily or in their common application – regulate general law enforcement activities that fall short of national security concerns (as defined rudimentarily by CJEU case law[10]), and could thus fall within the scope of the proposed spyware standards. Even when relevant national provisions formally address national security concerns, their routine application to general (non-national security) law enforcement activities would arguably bring the application of the law, or even parts of the law, under EU jurisdiction. If an intelligence law and its application relate strictly to matters of national security and therefore escape EU oversight, the following analysis of these laws remains relevant, since it identifies areas that warrant closer examination for compliance with the ECHR and potential breaches of discretion. Additionally, other law enforcement and criminal procedure laws mentioned in the sections below may well fall within the envisaged spyware standards' (still indeterminate) scope.

Greece

In Greece, the pertinent intelligence service – the National Intelligence Service (EYP) – and its practices were mainly regulated by the EYP Law 3649/2008 and the Freedom of Correspondence Law 2225/1994. Oversight of this service is primarily ensured by the Hellenic Authority for Communication Security and Privacy (ADAE), pursuant to Article 6(1)(a) of Law 3115/2003, and by the Greek Parliament's Special Permanent Committee on Institutions and Transparency, pursuant to Article 43A of the Rules of Procedure of the House (Decision No 2682/1987). While it is not clear whether Greece initiated the bill on Lifting of the Confidentiality of Communications and EYP Reform in the context of the Pegasus revelations,[11] it was adopted as Law 5002/2022 in the wake of

the scandal, replaced large parts of Law 2225/1994, and addressed several shortcomings in Greece's legal framework.

The European Parliament envisaged that the use of spyware should be authorised only in exceptional and specific cases in order to protect national security. In Greece, under Law 5002/2022, the confidentiality of communications may be lifted (i) for reasons of **national security** (as defined in Article 3), and (ii) in order to **investigate certain crimes**.[12] The latter does not require that the matter under investigation qualify as an issue of national security. As early as during the legislative procedure, the ADAE criticised that the proposed law would permit the lifting of communications' confidentiality for all felonies and for more than 50 misdemeanours. It also raised the law's incompatibility with Article 19 of the Greek Constitution owing to the multiple exceptions, effectively blurring the lines between the rule and the exception.

Parliament also stipulates ***ex ante* judicial authorisation** for spyware surveillance operations. This is mandated under Article 4(2) of Law 5002/2022 and Article 19(1) of the Greek Constitution. However, the lifting of confidentiality on the grounds of national security requires authorisation only from the prosecutor seconded to the EYP and a deputy prosecutor of the Supreme Court. A professor of constitutional law and former MEP (Kostas Chrysogonos, GUE/NGL, Greece, 8th parliamentary term) questioned this mechanism's constitutionality and ECHR compliance. This view is shared by the ADAE in its opinion on the draft law.[13] Lifting confidentiality to detect crimes is contingent on the approval of the competent Judicial Council, which consists of judges[14] and therefore ensures *ex ante* judicial authorisation, as requested by Parliament.

Furthermore, the law clarifies the conditions for the **surveillance of political figures** for reasons of national security. In this case, the threat to national security must be 'imminent and adequately substantiated', and authorisation is needed from the President of the Parliament for the process outlined above to continue. The law was criticised by the Greek National Commission for Human Rights for the divergent standards applicable to political figures and ordinary citizens. Nevertheless, many jurisdictions consider special protection of political figures necessary as a means of protecting the political process. This is also reflected in the European Parliament's spyware standards.

In cases relating to national security, the person concerned *must* be **notified** of the lifting of confidentiality 3 years after the procedure is complete, provided that the purpose for which the procedure was ordered is not compromised. However, according to the ADAE, it is not authorised to notify the person concerned before the 3-year non-disclosure period expires. First, the person surveiled must file a request, which is reviewed by a 'three-member body' consisting of two prosecutors and the head of the ADAE. Making a notification conditional on a request by the person surveiled would undermine the notification's purpose of transparency, since individuals are typically unaware of the surveillance and would not file a request unless they become suspicious. In addition, the Greek National Commission for Human Rights raised concerns about the 3-year period and the body's hierarchical composition. Professor of constitutional law Panagiotis Mantzoufas further raised bias concerns, as the individuals who decided to lift the confidentiality are also those who have to decide on the notification request. In cases relating to the investigation of crimes, the ADAE can, following the submission of a request and under certain conditions, inform the person concerned within 60 days (Article 6(8) of Law 5002/2022).

Article 7(4) of Law 5002/2022 regulates the post-surveillance **destruction of collected data** as requested by Parliament. Article 5 prescribes the deletion rules for national security surveillance.

The EYP's restructuring included the establishment of an Internal Audit Unit, with the aim to ensure compliance of the organisation's operation with legal requirements. However, as an internal body, this does not strengthen **independent oversight**, as requested by the European Parliament.

Spain

The main spyware scandal engulfing the government – known as CatalanGate – involved the Centro de Inteligencia Nacional (CNI) investigating Catalan separatists. The CNI is responsible for 'security

investigations', sometimes referred to as matters of national security, among other things covering territorial integrity. Three laws are particularly relevant in this context: Law 11/2002 establishing the CNI, Law 2/2002 on Prior Judicial Control of the CNI, and Law 9/1968 on Official Secrets. Most importantly, the Congressional Official Secrets Committee and the Ombudsman are tasked with oversight of the CNI. Following the scandal, the government announced various reforms, of which some have not yet been implemented. Meanwhile, the Basque Nationalist Party (EAJ-PNV) put forward a proposal that passed the Congress debate for consideration on 24 September 2024. It was subsequently sent to the competent committee, and the period for the submission of amendments was opened.

Overall, Parliament's PEGA committee report concluded that Spain has an independent justice system with sufficient safeguards; at the same time, it called for a legal reform to improve accountability and transparency.[15] While the Spanish Ombudsman confirmed the proper application of the **judicial authorisation** requirement, it indicated that judicial oversight could be improved, given the developments in surveillance technologies. Similarly, the PEGA committee was concerned that safeguards might be outdated and insufficient. Although it is not yet entirely clear what is envisaged, measures might include tightening approval criteria or enhancing *ex post* oversight,[16] given the intrusive nature of spyware. Others have **criticised** the law for its vagueness, with criticism possibly levelled at the unspecific criteria for judicial authorisation.[17] While the law defines the maximum **duration per authorisation** and makes extensions conditional on justification, the prolonged nature of the surveillance over years raised compliance and proportionality concerns. Civil society organisations believe that the operations were disproportionate, not least because of extensive relational targeting, including staff members and friends of Catalan MEPs. Conversely, one author contends that the operations were likely proportionate.

Regarding ***ex post* scrutiny** and **redress**, the Spanish legal framework is criticised by a media outlet for weak practical **oversight** by the Official Secrets Committee, for obstructing scrutiny by classifying relevant information as secret. Amnesty International criticised the absence of a **duty to notify**[18] the surveiled person after the intelligence operation is complete. Law 9/1968 on Official Secrets has become the focal point of discussions on *ex post* scrutiny. The CNI and its activities qualify automatically as classified information and are subject to confidentiality (Article 5(1) Law 11/2002). While confidentiality is not absolute, there is no timeframe for its expiration, meaning unless the information is declassified, it remains permanently secret. This prevents public scrutiny and effective redress. Critics regret the ineffective and slow legal proceedings. At least 47 allegedly targeted individuals lack information that would enable them to seek **remedies**. Others refute the CNI's responsibility.

Despite various unsuccessful attempts to **reform** the Official Secrets Law, the new government has announced a renewed effort as part of its democratic regeneration plan. The details are expected to be developed over the next 3 years. According to the government, the reform would improve citizens' insufficient access, to 'combine national security with the right to information and transparency'. Contrary to announcements, the government has not taken action to modify CNI regulations, so the EAJ-PNV put forward a proposal to that end. Its main purpose is to improve political and judicial control over the CNI: its director would be chosen directly by the head of government to assume political responsibility. It also proposes a greater parliamentary control through the Official Secrets Committee, which was criticised by the media for failing to convene during 3 years, and for its members not being adequately informed by the CNI. The proposal would also tighten prior judicial authorisation for surveillance measures from one single Supreme Court judge to three Supreme Court judges deciding it. Furthermore, it would explicitly mention the proportionality requirement as a criterion for judicial authorisation.

Given that the EU generally lacks the competence to regulate national security matters and Parliament suggested relying on Treaty provisions relating to 'judicial cooperation in criminal matters' as a legal basis for its spyware standards, it is important to take stock of Spain's 2015 amending its **Criminal Procedural Law**. Spain is one of the few EU Member States that explicitly

permits and regulates the use of spyware by law enforcement authorities. The 2015 reform introduced rules on the remote search of computers and other electronic devices (Article 588 septies a of Law 13/2015). These may be carried out only in the context of a criminal procedure and with prior judicial authorisation. Article 588 specifies the offences for which the remote search of information technology (IT) devices can be authorised. It requires compliance with the principles of adequacy, necessity and proportionality. Thus, this law meets some of the key spyware standards envisaged by Parliament's recommendation. Nevertheless, it does not stipulate a duty to notify individuals after remote computer searches, while it does so for intercepting communications.

Hungary

In Hungary, the relevant intelligence service and its practices are regulated by the CXXV Act of 1994 on the national security services (National Security Services Act, NSSA).[19] The NSSA applies where covert information gathering is used for national security[20] and other purposes (Sections 4-9 NSSA). The Specialised National Security Service used Pegasus in its capacity as the central service provider for national security and law enforcement agencies. It supported the activities of an undisclosed organisation, authorised to conduct covert intelligence gathering.

Although the NSSA was modified 27 times during the past 8 years, none of the amendments implemented the European Parliament's June 2023 country-specific recommendations, aiming to give better legal guarantees for the protection of private life.[21] Instead, the most recent change introduced an integrity test ('reliability test', initially intended to prevent and detect corruption crimes) for almost all government employees, to assess their behaviour in artificially created scenarios.

The Parliamentary Committee on National Security is the key **oversight** body in Hungary (Section 14 NSSA). The committee has monitoring and fact-finding powers, including the power to examine complaints alleging the illegality of surveillance operations,[22] but it cannot directly remedy violations (Sections 14-19A NSSA). The ECtHR does not view the Data Protection and Freedom of Information Authority (NAIH) as an effective oversight body ensuring adequate redress, owing to limitations on its scope of investigations.[23]

Under the NSSA, some covert means are subject to external authorisation (Sections 56-60 NSSA), while others are not (Sections 54 and 55 NSSA).[24] Section 56 a) to e) NSSA only provides a broad list of special surveillance techniques that are subject to **external authorisation** by either the President of the Metropolitan Court or the Minister of Justice. While spyware is not explicitly mentioned, Pegasus was apparently understood as falling within the scope of Section 56, and its use thus required authorisation from the Minister of Justice (Section 58(2) NSSA). This appears not to be in line with the European Parliament's spyware recommendation. In a 2016 judgment,[25] the ECtHR found that the political nature of a minister's authorisation increases the risk of abusive measures, and that such an approval does not provide the necessary guarantees of independence, impartiality and a proper procedure. In the same vein, the legitimacy of the delegation of power to the secretary of state to the Ministry of Justice is also subject to controversy.

According to the NAIH, 'Hungarian law in force does not differentiate between professions and professional activities [e.g. 'journalist, human rights activist, opposition politician, lawyer and businessman'] with regard to the conditions for using covert information gathering subject to external authorisation'. In its recommendation, Parliament indicates that politicians may warrant special protection, and that related data 'must not be sought through spyware unless there are sufficient grounds, established under judicial oversight, confirming involvement in criminal activities or national security matters'.

Section 58(4) NSSA stipulates that the secret collection of information is authorised for a **duration** of 90 days, which can be extended by another 90 days. The law's wording is unclear on whether surveillance permission can be extended multiple times, leaving authorities with broad discretion.

Hungarian law does not oblige the intelligence agency to **notify** the aggrieved parties after the intelligence operation's completion that they have been subject to surveillance. Much to the contrary, Section 58(6) NSSA explicitly provides that the person concerned not be informed. In its *Szabó and Vissy* v *Hungary* and *Hüttl* v *Hungary* judgments, the ECtHR noted further shortcomings including insufficient **redress**; at the time of writing, Hungary has not addressed these shortcomings, despite having announced a bill for spring 2023.

Indicative of a broader trend, there are growing concerns about the potential misuse of the LXXXVIII Act of 2023 on national sovereignty protection, notably for political repression and the chilling effect it may have on political participation. While the act does not permit covert intelligence gathering, it grants the Sovereignty Protection Office (SPO) the power to inquire about attempts to influence public opinion, including through media and private organisations or companies allegedly financed from abroad. According to Hungarian non-governmental organisation TASZ, it can be safely assumed that the SPO might claim that any public manifestation or event serves foreign interests and therefore threatens Hungary's sovereignty.

Poland

In Poland, the 1990 Police Act provides the legal basis for operational surveillance activities of the police, while the 'competence laws' are the basis for such activities of the respective 'special services' (the term used for secret services in Polish legislation).[26] The latter designation is ambiguous, encompassing three distinct categories of services: intelligence services, intelligence and police services, and police services.[27] These include the Central Anti-Corruption Bureau (CBA), the Military Counterintelligence Service (SKW), and the Internal Security Agency (ABW) – the three agencies with documented use of the Pegasus spyware.[28] The CBA and the ABW are difficult to distinguish from specialised law enforcement agencies.

Oversight is exercised by multiple entities, including the Prime Minister, the Minister Coordinator for Special Services, the Supreme Audit Office, the Ombudsman, the President of the Office for Personal Data Protection, and the Parliament. Within the Parliament, in principle, the **oversight** responsibility falls to the Special Services Committee of the lower chamber of the Parliament (the *Sejm*). However, because of its political capture prior to the October 2023 elections, deputies formed the Senate Special Committee on Surveillance in the opposition-controlled upper chamber of the Parliament (Senate). It made best efforts to investigate the Pegasus scandal, despite lacking investigative powers. After the current government took office, an investigation committee was set up in the *Sejm*; its works are still ongoing.[29] However, Poland does not seem to have invited Europol to investigate spyware abuse, as recommended by the European Parliament.

While courts perform *ex ante* scrutiny, the existing **judicial authorisation** procedure has been characterised in the PEGA committee report as a mere way of giving surveillance for political purposes an appearance of legality. In its highly anticipated ruling of May 2024, the ECtHR held that the Polish legislation (notably the Police Act as amended in 2016, and the 2016 Anti-terrorism Act) 'did not provide sufficient safeguards against excessive recourse to surveillance and undue interference with individuals' private life', and 'the absence of such guarantees was not sufficiently counterbalanced by the existing mechanism for judicial review'. These laws are still in force. The government is currently working on a draft 'Code of Operational Work'.[30] The draft strengthens *ex ante* judicial control by requiring that the courts rule in sessions attended by a prosecutor and a secret service representative, providing justification for both approval and denial of requests (unlike the current system). The draft also decentralises the competence for authorisation across 11 district courts in different appellate jurisdictions, thereby reducing the workload on the District Court in Warsaw.

The functioning of the **oversight** mechanisms no longer appear to be a problem. For example, there are no more reports of non-respect for the statutory powers of oversight bodies, such as the Ombudsman and the Supreme Audit Office. Moreover, the 2024 EU Rule of Law report noted a 'significant progress on continuing efforts to ensure functional independence of the prosecution

service from the Government'. However, the system with an opposition member presiding over the parliamentary Special Services Committee, in place until 2016, was not reinstated with the appointment of the new composition of this committee. Moreover, no action has been taken to meet Parliament's recommendation to implement the EU Law Enforcement Directive (EU) 2016/680 in a manner that would ensure the data protection authority has the power of supervision over the processing of personal data by secret services (CBA and ABW).[31]

The above-mentioned 'Code of Operational Work' would introduce **post-factum notification**, requiring that individuals subjected to operational surveillance be informed within a year of its conclusion, allowing them to file a complaint with the court that authorised the surveillance. Such provisions address Parliament's concerns about the modalities of effective *ex post* scrutiny of surveillance activities.

As regards **effective redress**, the new government has focused on addressing systemic issues with a view to restoring the independence of the judiciary. In February 2024, it presented to the General Affairs Council an action plan specifying the steps to be taken to address persistent concerns in this respect. In May 2024, the European Commission concluded there was no longer a clear risk of a serious breach of the rule of law in Poland, and closed the procedure under Article 7(1) TEU.

In July 2024, the Polish Parliament adopted a law on the National Council of the Judiciary (NCJ), followed, in September 2024, by a law on the Constitutional Tribunal. The two laws seek to address, among other things, the problem of 'neo-judges' (judges appointed or promoted on the request of the politically captured NCJ). The President did not sign these two laws and decided to refer them to the Constitutional Tribunal for preventive review. A draft bill separating the office of the Minister of Justice from that of the Prosecutor General is being processed by the Council of Ministers.

The action plan mentioned above envisages establishing an institutional system for the implementation of ECtHR judgments. The government has already taken corrective action regarding the revision of Poland's positions in proceedings before the CJEU. Moreover, a review is ongoing of the positions, recommendations, and objections expressed by the EU institutions.[32]

The investigation of the Pegasus scandal renewed concerns about the constitutionality of the 2016 **criminal procedural** provision undermining the 'fruit of the poisonous tree doctrine'. Arguably, the design of Pegasus made its use illegal by design under Polish law.[33] Under traditional doctrine, such illegally collected evidence would be inadmissible in court. However, in 2016, the Code of Criminal Procedure was revised to specify that, with some exceptions, 'the evidence cannot be deemed inadmissible solely on the grounds that it was obtained in violation of procedural regulations or by means of a prohibited act' (Article 168a). The courts and legal doctrine have struggled to find a Constitution-compliant interpretation.[34] The Members of Polish Parliament proposed a draft bill to repeal the controversial Article 168a in line with calls from the European Parliament.

ENDNOTES

1 Additionally, the Commission recently published its guidance on the export of cybersurveillance items.

2 The assessment, based on desk research, is not meant to be exhaustive. It focuses primarily on the legal framework; practical implementation may vary, and additional regulations including subordinate laws and soft law may also apply.

3 In its recommendation, Parliament considers that the *use* of spyware for national security purposes may only be regulated indirectly through, for example, fundamental rights and rules relating to data protection. Drawing on the rationale of the CJEU's case law on data retention, it can be argued that the data protection *acquis* applies where 'communication service providers are ordered to cooperate with State authorities in the installation and use of spyware' for national security purposes. In the same vein, involving commercial spyware vendors in national security surveillance operations may bring a public-private surveillance operation and/or the regulatory framework under the scope of EU data protection rules and EU fundamental rights. Notably, when commercial vendors retain significant discretion without close governmental oversight, the commercial orientation may be seen as prevailing – even within public-private intelligence operations. The opposing view could argue that taking unfettered advantage of intelligence outsourcing falls within the scope of 'safeguarding national security', thereby excluding any EU competence under Article 4(2) TEU.

[4] Additionally, Parliament calls for regulating the placing on the market of spyware based on Article 114 TFEU. This aspect falls outside the scope of this briefing.

[5] D. Kaye, The impact of spyware on fundamental rights, Testimony to the PEGA committee (22 October 2022), p. 5; UN Special Rapporteur D. Kaye, Surveillance and human rights, A/HRC/41/35, 28 May 2019, pp. 7-9.

[6] G. Sartor and A. Loreggia, The impact of Pegasus on fundamental rights and democratic processes, pp. 36-44, p. 42; ECtHR Research Division, National security and European case-law, 2013; CoE AS/Jur Committee, Pegasus and similar spyware and secret state surveillance, September 2023, pp. 20-26; CoE Commissioner for Human Rights Dunja Mijatović, Highly intrusive spyware threatens the essence of human rights, January 2023. On bulk data interception, see I. Brown and D. Korff, Exchanges of Personal Data After the Schrems II Judgment, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, 2021, pp. 45-54 (p. 52).

[7] Parliament seems to envisage high standards that would prohibit the use of spyware within the scope of the EU's competences for law enforcement. Roughly speaking, spyware should only be used for law enforcement purposes if the criminal activities amount to a matter of national security. However, genuine cases of national security are excluded from the scope of EU competences.

[8] These may include far-reaching data collection; conflicts of interest of contractors (spyware vendors catering to adversarial customers); misuse of data by contractors (who control the servers and whose actions may escape traditional control and oversight mechanisms); misuse of spyware by operators (who may not face resistance by controllers); evidence tampering and unauthorised copies (owing to an operator's control of the device and data flows); and non-disclosure of security vulnerabilities despite over-riding public interest.

[9] The sections on Member States' legislation were drafted with the help of Piotr Bąkowski (Poland) and Mar Negreiro (Spain), policy analysts in the Members' Research Service.

[10] See Annex I in H. Mildebrath, Europe's PegasusGate: Countering spyware abuse, EPRS, European Parliament, 2022.

[11] FRA, Greek country report: 2023 update of the study on surveillance by intelligence services, pp. 10-11.

[12] Articles 254(1)(d) and 255(1)(b) of the Criminal Procedure Law 4620/2019 specify that lifting confidentiality for investigating certain crimes must be done in compliance with Articles 6, 8 and 48(2) Law 5002/2002.

[13] FRA, Greek country report: 2023 update of the study on surveillance by intelligence services, p. 7, referencing the ADAE.

[14] On the jurisdiction and composition of Judicial Councils, see Articles 3-11 Criminal Procedure Law 1620/2019.

[15] The information relating to the situation of spyware surveillance in Spain, pointed out by the May 2023 PEGA committee report and the June 2023 European Parliament country-specific recommendations, is still accurate. During the period observed, no significant legislative reforms were adopted, although several proposals were put forward.

[16] Critical of *ex ante* judicial oversight, J. L. González Cussac, 'Intromisión en la intimidad y Centro Nacional de Inteligencia. Crítica al modelo español de control judicial previo', *Revista Penal México*, 2015, No 8, pp. 91-92.

[17] Additionally, the relevant laws stipulate at best implicitly the requirement of proportionality for national security-related intelligence operations. By contrast, this requirement is clearly articulated in criminal procedural law (e.g. Art. 588 of Law 13/2015) and recognised explicitly by both the Spanish Constitutional Court and the Supreme Court for law enforcement activities (Constitutional Court rulings STC 49/1999 of 5 April 1999; STC 126/2000 of 16 May 2000; and 239/2006 of 17 July 2006).

[18] The ECtHR usually does not require both *ex ante* and *ex post* judicial oversight (para. 77). In favour of extending notifications to matters concerning national security, see A. J. Alfonso Rodríguez, 'Gobernanza democratica y rendicion de cuentas: control judicial de las actividades de inteligencia (ODS 16.6)', *Revista de Derecho de la UNED*, 2023, Vol. 31, pp. 55–111.

[19] For other laws on covert information gathering for law enforcement purposes, such as the XXXIV Act of 1994 on the Police (in particular Sec. 70 et seq.) and the XC Act of 2017 on criminal procedure (in particular Sec. 231 et seq.), see NAIH, Findings of the investigation of the NAIH, launched ex officio concerning the application of the 'Pegasus' spyware in Hungary, NAIH-423-2/2022, 31 January 2022, pp. 8-10.

[20] 'National security interest' is defined in Sec. 74(a) NSSA.

[21] For an overview of most of these amendments, see FRA, Hungarian country report: 2023 update of the study on surveillance by intelligence services, pp. 9-11.

[22] Section 14(4)(c) NSSA presupposes that the complainant rejects the outcome of a prior complaint to the competent minister, i.e. the Minister of the Prime Minister's Cabinet Office, implying a multi-tiered oversight structure.

[23] FRA, Hungarian country-report: 2023 update of the study on surveillance by intelligence services, pp. 13-15; ECtHR judgment in Case with application no 58032/16, *Hüttl* v *Hungary*, 29 September 2022, paras. 16-18.

[24] In a similar vein, judicial authorisation is mandated for some forms of covert information gathering for law enforcement purposes (Sections 70-72 Police Act), while it is not prescribed for others (Sections 66-69 Police Act). In some instances, authorisation by the Minister of Justice is needed (Sec. 63(7) Police Act). The use of measures requiring judicial authorisation may be approved for up to 90 days at a time, subject to extension upon the submission of a new request (Sections 75/B(1) Police Act). Sometimes even significantly longer (Sections 75/B(2) Police Act). The Police

Act stipulates a notification duty in Section 75/D(5), a deletion obligations in Section 75/H, and a retention period in Section 91/A(1a). See also Section 214 and in particular Section 231 et seq. XC Act of 2017 on criminal procedure.

25 The judgment concerns the legal basis for anti-terrorism surveillance, but incidentally addresses the relevant NSSA provisions.

26 See Article 19 of Ustawa z dnia 6 kwietnia 1990 r. o Policji, *Journal of Laws* 1990, no 30, item 179; Article 17 of Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, *Journal of Laws* 2006, no 104, item 708; and Article 27 of Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, *Journal of Laws* 2002, no 74, item 676. Such operational surveillance may include 'obtaining and preserving data contained in data storage devices, telecommunications end devices, as well as in IT and telecommunication systems'.

27 M. Kolaszyński and G. Małecki, 'Intelligence Oversight and Accountability in Poland: Has Anything Changed?', *International Journal of Intelligence and CounterIntelligence*, 2024, preprint, pp. 1–29.

28 According to information from the Prosecutor General sent to the *Sejm* and Senate, 578 people were subjected to operational surveillance using Pegasus between 2017 and 2022.

29 Moreover, the Prosecutor General appointed a team of specialised prosecutors to examine the legality of the activities carried out using Pegasus. The team has been tasked with all Pegasus-related investigations, including the one concerning the alleged abuse of authority and failure to fulfil duties by public officials, and the investigation into the purchase of Pegasus software using the 'Justice Fund' (Fund for Victim and Post-Penitentiary Assistance).

30 See SSP Iustitia, Opinia Zarządu SSP Iustitia w sprawie projektu ustawy – Kodeks pracy operacyjnej, December 2023; For a critical perspective on the draft, see P. Opitek, Miało być lepiej, może być gorzej. Kilka uwag do projektu Kodeksu pracy operacyjnej, May 2024.

31 No relevant amendment has been made to the law that implemented the directive (Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, *Journal of Laws*, 2019, item 125).

32 Ministry of Justice, Minister Sprawiedliwości przedstawił Plan Działań Polski ws. przywracania praworządności, press release, 20 February 2024.

33 It is argued that Pegasus's design – which provides for the sharing of data with third parties outside Polish territory and does not preclude a possibility of tampering with the data stored on the infected device – renders it impossible for this type of spyware to be used legally in Poland. This is because the spyware's functionalities make it ineligible for teleinformation security accreditation by the Internal Security Agency or the Military Counterintelligence Service, required for systems in which classified information is processed. See Senat Rzeczypospolitej Polskiej, Komisja Nadzwyczajna ds. inwigilacji przyjęła raport ze swoich prac, September 2023 (see bottom of the page for access to the report), pp. 33-34; A. Barczak-Oplustil et al., Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasusa), 2022; M. Bidziński, Ocena legalności i skutków prawnych działań podejmowanych przy użyciu systemu Pegasus, 2022.

34 See e.g. K. Lipiński, 'Glosa do wyroku Sądu Apelacyjnego we Wrocławiu z 27 kwietnia 2017 r., II AKa 213/16', *Palestra*, Vol. 10, 2017.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)