Third-party intervention in the case of Marton Dániel ASBÓTH and Others against Hungary (app. no. 38155/22) by Irídia — Centre for the Defence of Human Rights, Gesellschaft fur Freiheitsrechte (GFF), Data Rights, Homo Digitalis and Panoptykon

Dear Madam or Sir,

1. We are grateful for invited us to give our perspective on the following question: Does the possibility that the applicants could be subjected to secret surveillance without external/judicial control represent an unjustified/disproportionate potential interference with their rights under Article 8 (see, mutatis mutandis, Szabó and Vissy v. Hungary)

2. To this question we all answer yes, and have decided to articulate our brief towards providing arguments to detail our perspective, looking first at the requirements for authorisations, then a posteriori measures and thirdly, notifications requirements. Additionally, we have chosen to bring to this court's attention a pattern we see regarding the types of victimes of abuse.

I) Safeguards required

3. This first section is focused on the question addressed to us by your court, that is, to provide our perspective on core measures meant to balance out the power for States to rely on secret surveillance. For this reason, the reader will firstly be bestowed an understanding of how the requirement for authorisations is provided for in countries, legally and in practice. After this, a case study on German rules applying to a posteriori mechanisms established to safeguard fundamental rights of citizens. Last but not least, the notification requirements required in the case law of this court as well as the Court of Justice of the Europeans Union (CJEU) will be developed to be confronted to our pending cases.

A) Authorisations

4. With regards to authorisations, we find that the state of safeguards across the countries we are reporting from is inconsistent and unadapted to new technologies.

5. Indeed, in Roman Zakharov v. Russia (47143/06), this Court has consistently emphasised that effective safeguards against abuse are in-

dispensable in the context of secret surveillance. The Court has explained that Article 8 safeguards require oversight of surveillance mechanisms by independent and impartial decision-making bodies, ideally judicial, […].

6. Yet as prescribed below, countries in which the PEGA coalition seeks the accountability of the State for spyware infections do not show signs of alignment with the quality of oversight required by the Court. Furthermore, our Coalition notes that despite the ECtHR observing in the Zakharov case that "[i]t is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure", in practice this gold standard can fall shot in the context of potent emerging technologies.

POLAND

7. For instance, in Poland judicial authorisations are required. Yet despite this requirement and judges actually having been put in a position to authorise or refuse the infection of individuals' phones with the Pegasus spyware, safeguards failed to prevent citizens from the depth of the surveillance scandal still shaking the country. For more details on the case please see our intervention in the Brejza case (n°27830/23) currently pending before your court. To add more details on authorisations in Poland, we found through a senior EU official[1] that Polish judges have explained that the capabilities of the surveillance measures they were authorising had been misrepresented to them, leaving them feeling instrumentalised in violations. Therefore we recommend that any surveillance technique authorisation is required to bear the clear explanation of the type and amount of data to be collected, as well as the implications on individuals' privacy. Authorisers must be put in a position to understand the capabilities and consequences of techniques they authorise. This point is further supported by requirements found in German law, as detailed below.

GERMANY

8. In Germany, the Federal Constitutional Court has established that covert surveillance measures by domestic intelligence services constituting serious interferences with fundamental rights are subject to a requirement of prior authorisation by an independent body. This re-

[1] From 38th minute on, CPDP, May 2025, panel of spyware and cybersecurity with GFF, Data Rights, cybersecurity expert Sven Herping, former MEP Sophie in 't Veld and Mme Buchta, Closing the Digital Backdoor: Strengthening Vulnerability Management to Combat Spyware, May 21st, 2025

quirement flows directly from the principle of proportionality and serves as a structural safeguard against arbitrary State action (Judgment of 26 April 2022, 1 BvR 1619/17, paras. 214 et seq.; Judgment of 27 February 2008, 1 BvR 370/07, paras. 257 et seq.).

9. Specifically, the Court held that where a covert surveillance measure gives rise to a serious interference with fundamental rights – such as covert access to an information technology system – prior review by an independent body is constitutionally required, since the affected person would otherwise be left entirely without protection. The legislature retains discretion regarding the precise design of such review, including the choice of the authorising body and the applicable procedure, but the independence of the reviewing body from the investigating authority is a non-negotiable constitutional prerequisite (Judgment of 27 February 2008, 1 BvR 370/07, paras. 257–261); the independent authorising body must furthermore be comprehensively informed of the state of affairs (Judgment of 26 April 2022, 1 BvR 1619/17, para. 215). A point that echoes the shortcoming expressed by Polish judges, that were not empowered with the understanding of what type of surveillance they were required to authorise or prevent.

10. Prior authorisation by an independent and neutral body constitutes a significant element of effective fundamental rights protection, since the affected person is unable to assert their own interests in advance due to the covert nature of the measure. Prior review thus serves the function of 'compensatory representation' of the affected person's interests in the administrative procedure (ibid.). Any body entrusted with this function must offer the same guarantees of independence and neutrality as a court, and must give reasons for its assessment of lawfulness (ibid., para. 260); exceptions for urgent cases are permissible only if prompt subsequent review by the independent body is guaranteed (ibid.).

11. However, the interveners submit that judicial authorisation alone cannot satisfy the constitutional guarantee of effective ex-ante control in the context of modern surveillance software. Under German law, the constitutional distinction between source telecommunications surveillance – limited to intercepting ongoing communications – and a full remote search of an information technology system requires not only different legal thresholds, but also distinct technical configurations of the software deployed. A court authorising the deployment of such software is, in practice, not equipped to verify whether the technical means actually comply with these requirements. Courts must rely on the representations of the investigating authorities, and cannot reasonably be expected to conduct an independent technical assessment of the surveillance software – particularly where that software is

obtained from a third-party commercial provider whose full functional scope may be unknown even to the deploying authority itself. Which is typically the case for potent spyware procured externally. Relying on the representations of investigators, however, runs counter to the constitutional requirement that the independent body must form its own independent judgment as to whether the requested covert surveillance measure meets the statutory conditions (Judgment of 26 April 2022, 1 BvR 1619/17, paras. 215). The risk is therefore not merely theoretical: where software capable of conducting a full remote search is deployed under a warrant authorising only source telecommunications surveillance, the judicial authorisation provides no meaningful protection against a far more intrusive interference than the one sanctioned. The interveners therefore submit that an independent technical review of the surveillance software by a neutral body – such as a data protection authority or a specialised technical agency – prior to its deployment is a constitutional necessity. A judicial warrant issued without such prior independent certification cannot, by itself, satisfy the constitutional requirements of effective ex-ante control.

SPAIN

12. In Spain the use of the Pegasus spyware, has been linked to intelligence activities allegedly carried out by the Spanish National Intelligence Centre—hereafter, the CNI.

13. The CNI is mainly regulated by Law 11/2002 of 6 May, regulating prior judicial control of the CNI; and, as regards classification and official secrecy, by Law 9/1968 of 5 April, on Official Secrets. Law 9/1968 allows classifying information as secret if its disclosure could harm national security or defense. In practice, this has been used to restrict access to intelligence-related information and, notably, to prevent individuals from receiving adequate explanations about possible State surveillance—even when courts investigating criminal cases request that information.

14. Article 5 of Law 11/2002 broadly classifies as secret virtually all CNI-related information. This classification severely hinders effective external oversight by both affected individuals and institutional supervisory mechanisms.

15. Article 2.2 states that the CNI is overseen by Parliament's Official Secrets Committee, but this oversight is largely symbolic due to legal limits and the CNI's unilateral power to classify information. During the XIV Legislature, the Committee met only once—prompted solely by the CNI Director's appearance regarding the Pegasus scandal—highlighting its inability to conduct meaningful investigations or disclose

information to clarify surveillance operations or aid ongoing criminal cases.

16. Prior judicial control under Organic Law 2/2002 requires the CNI's Secretary of State Director to obtain authorisation from a Supreme Court judge for measures affecting home inviolability or communication secrecy, where necessary for CNI functions. However, this ex-ante control has significant structural limitations. The regulation is extremely brief, concentrating judicial authorisation in a single provision without defining: the material scope of authorised measures; necessity and proportionality criteria; individualisation of affected persons; technology used; categories of interceptable or extractable data; or specific safeguards for particularly intrusive surveillance, such as infecting mobile devices with spyware containing powerful hacking tools.

17. The Spanish experience shows that formal judicial authorisation alone is not a sufficient safeguard. The Irídia case involves a lawyer allegedly surveilled with Pegasus without judicial authorisation. Similarly, in the case of the former President of the Government of Catalonia, part of the surveillance purportedly had judicial authorisation, while another part did not.

18. The law allows judicial authorisation for an initial three months, with possible extensions. However, the legal framework lacks clear limits on those extensions and fails to provide robust mechanisms for periodic review or active judicial monitoring. In practice, this enables secret surveillance to be prolonged without adequate scrutiny of its ongoing necessity and proportionality.

B) A posteriori control mechanisms

GERMANY

19. The German Federal Constitutional Court has established that the principle of proportionality, read in conjunction with the guarantee of effective legal protection under Article 19(4) of the Basic Law, imposes comprehensive requirements on the design of any covert surveillance regime with regard to transparency, individual legal protection, and independent oversight (Judgment of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09, para. 134; Judgment of 19 May 2020, 1 BvR 2835/17 para. 214). These requirements are not merely procedural in nature; they are a direct expression of the fundamental rights at stake. Since covert surveillance measures preclude affected persons from asserting their rights in advance, ex-post safeguards serve as the pri-

mary–and often the only–means by which the substance of those rights can be vindicated.

20. Because transparency and individual legal protection can only be ensured to a very limited degree in the context of covert surveillance measures, the guarantee of effective independent oversight assumes a compensatory constitutional function (Judgment of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09, para. 140). An independent oversight body vested with effective powers is constitutionally required (Judgment of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09, para. 141; Judgment of 19 May 2020, 1 BvR 2835/17 para. 281; Judgment of 24 April 2013, 1 BvR 1215/07, para. 215; Judgment of 26 April 2022, 1 BvR 1619/17, para 290). All data collection must be fully logged and made available to the oversight body in a practically evaluable form (Judgment of 24 April 2013, 1 BvR 1215/07, para. 215; Judgment of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09, para. 141). Given this compensatory function, regular oversight at appropriate intervals – not exceeding approximately two years – is constitutionally mandated (Judgment of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09, para. 141; Judgment of 24 April 2013, 1 BvR 1215/07, para. 217).

Spain

21. The Spanish framework lacks sufficient safeguards for ex-post control of CNI secret surveillance. Once a measure is authorised and implemented, the law does not clearly establish an independent, effective, and accessible system for subsequent review to verify whether the interference remained within authorised limits, continued to be necessary and proportionate, and whether data were handled with adequate safeguards. This deficiency is aggravated by the secrecy regime under Law 9/1968 and Article 5 of Law 11/2002.

22. In Spain, criminal proceedings offer the greatest investigative capacity in principle, as courts can request information often inaccessible elsewhere. However, even investigating courts face severe limits due to the official secrets regime and the general classification of CNI activities. The only way to access such information is declassification by the Council of Ministers. This avenue does not constitute an effective mechanism of judicial control. Although an investigating judge may theoretically request declassification, in practice it depends on a political decision without clear criteria. If declassification is refused, a contentious-administrative appeal may be lodged before the Supreme Court, but such review is limited to formal legality—not whether the classified information reveals an unlawful or disproportionate interference with fundamental rights.

23. As a result, even when technical evidence of spyware infection exists, access to essential information remains restricted. At most, the CNI may only confirm whether surveillance occurred, without revealing its scope, duration, data affected, subsequent use of information, or limits applied to tools like Pegasus. Consequently, there is no genuinely effective procedure for reviewing potential unlawful acts of State espionage carried out through the intelligence agency.

24. These limitations also affect the investigation of those responsible. The Official Secrets Act prevents current and former CNI Directors from fully answering questions from judicial bodies or parties to proceedings. The former CNI Director—currently indicted in several criminal investigations—stated before a judicial authority that she could not testify freely due to this legal regime.

25. Spain's cybercrime prosecution office has failed victims of State surveillance by systematically opposing investigations and seeking their dismissal. Likewise, the Ombudsperson—the only body with access to classified CNI information—cannot disclose any content, and its sole intervention in the Pegasus case was early and ineffective, failing to clarify the spyware operation or establish ongoing oversight.

C) Notification

26. Given the lack of robust compliance with the safeguards discussed, the question of ex-post notification may become a central one to ensure that citizens keep a sens that they can hold their country accountable.

27. In line with European Court of Human Rights (ECtHR) caselaw, ex-post notifications can only be omitted where the oversight body, available remedies and procedural safeguards are strong. Indeed, in Association Confraternelle de la presse c. France et alia (49526/15), 2025, the ECtHR sets clearly that if these three conditions are not met, ex-post notification is due. The PEGA coalition favours the strong position taken by the Court of Justice of the EU (CJEU) in 2020 on the matter (see below), as it otherwise becomes a thorny hurdle to discuss the details of the implementation of all three conditions, which is always at the disadvantage of targeted citizens given resources of States. Our observation is built on the fact that in multiple of the countries we are reporting from, all three conditions were not met and yet individuals we work with have not received any notification. For details on the definition of such conditions see for instance Roman Zakharov v. Russia (47143/06).

28. The CJEU has indeed gone further in its requirement for notifications in its ruling on the joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier ministre and Others and Ordre des barreaux francophones et germanophone and Others v. Conseil des ministres [GC], 6 October 2020. the La Quadrature du Net ruling of 2020 created in its paragraphs 190 and 191 an explicit obligation for States to notify individuals after they are no longer deemed a threat and surveillance has ceased.

29. Multiple Pegasus infection cases supported by members of the PEGA Coalition took place a few years after this CJEU ruling and should have imposed a notification of individuals. Yet none of these individuals were notified, either in Spain, Hungary or Poland. Poland appears to be looking to become compliant now that the government has changed, as it recently issued notifications. This goes to confirm that critical EU safeguards set up to uphold individual's rights to an affective remedy are currently being ignored by States. Through interactions we have had with institutional contacts we were informed that some intelligence services claim that sending notifications to individuals could be too burdensome operationally. We will never accept this claim and refute it entirely. The onus is on the State to ensure it upholds the most fundamental rights of citizens, especially for situations that impact their mental health and behaviour. Generic emails would be a first step in the right direction to empower citizens and start rebuilding trust.

30. In a nutshell, as organisations supporting investigative journalists that were infected because they were investing corruption cases and lawyers targeted for their communications with their clients, we see notifications are one of the only requirements to offer real tangible agency to citizens that that feel defenceless vis-à-vis States' powers. For detail on the behavioural impact of the fear of surveillance, please refer to Data Right's intervention in case Javadov, Ganbarova and Other vs Azerbaijan (appl. 45877/22 and 30573/22) currently pending before your court.

GREECE

31. Greece exemplifies how even potentially effective remedies can be systematically undermined. The subsequent notification system operated by the Hellenic Authority for Communication Security and Privacy (ADAE) was retroactively abolished for surveillance conducted on national security grounds after journalist Thanasis Koukakis sought confirmation of his monitoring by the National Intelligence Service (EYP). Although the law was later amended again, individuals must still wait three years before requesting information, and even then,

they are only informed of the duration — not the justification — of the surveillance. A three-member committee, including the prosecutors who originally authorised the interceptions, decides on disclosure, raising serious concerns about impartiality.

32. Further eroding safeguards, a 2023 Supreme Court opinion barred ADAE from investigating mobile providers after surveillance requests, threatening criminal sanctions for such inquiries—one government organ effectively emptying out the potential remedy provided by another. Meanwhile, data protection reforms have further weakened oversight, stripping the Greek Data Protection Authority (DPA) of its ability to oversee intelligence-related data processing.

SPAIN

33. In Spain, there is no effective mechanism for notifying persons affected by secret surveillance after the fact, meaning that individuals do not have a clear and effective right to be informed once the surveillance has ended and notification no longer risks undermining its legitimate aim.

34. This absence of notification has serious consequences. Without it, affected persons cannot know they were subjected to surveillance, and therefore cannot challenge the measure, seek judicial review, request destruction of unlawfully obtained data, or obtain redress. As a result, the lack of subsequent notification deprives individuals of their rights of defence and access to an effective remedy.

35. The absence of any official notification has meant that surveillance victims only learned of the facts through reports from international organisations, specialised laboratories, or private companies like WhatsApp. It was WhatsApp's notification to 1,400 users—including two elected representatives of the Government of Catalonia, whose cases remain open—about Pegasus infections on their devices that prompted the forensic examination leading to the case.

36. This deficiency was highlighted in the so-called "Catalangate" case, documented by the Citizen Lab in April 2022 and confirmed by Amnesty International, which revealed the surveillance of 65 individuals linked to the Catalan independence movement between 2015 and 2020. Notably, additional reports filed at the national level within the proceedings corroborated the initial findings and conclusions of the Citizen Lab.

37. This situation demonstrates that in Spain, access to critical information only depends on external, random, or private disclosures. Euro-

peans depend on forensic research of a university in Canada to access redress.

38. Following the scandal and a closed-door meeting of the Official Secrets Committee, it was leaked that the CNI allegedly acknowledged spying on 18 persons with Supreme Court authorisation. However, the Government has never publicly confirmed this or provided full explanations. The Irídia case concerns one of 47 persons allegedly spied upon without judicial authorisation, who to this day have received no official information about what happened to their phones, what data was obtained, how it was used, how long surveillance lasted, or whether the data was destroyed.

II) Patterns with targets & remedies

39. In all cases compiled within the present intervention, evidence reveals a pattern: State espionage via military-grade spyware like Pegasus does not indiscriminately target private individuals. Instead, it deliberately and systematically targets specific profiles.

40. Targeting has focused on individuals performing critical functions in a democratic society: journalists, lawyers, human rights defenders, political leaders, and opposition parliamentarians (national and European). These affected persons require reinforced protection under the ECHR. Surveillance of journalists may compromise source confidentiality, press freedom, and their oversight role. Surveillance of lawyers may affect legal privilege, client confidentiality, and defence rights. Surveillance of parliamentarians and political leaders may harm political pluralism, representative freedom, and the functioning of democratic institutions.

41. This kind of interference cannot be viewed solely as an individual privacy violation. When State espionage targets lawyers, journalists, human rights defenders, and political representatives, its impact extends beyond the individual and undermines the structural safeguards of the rule of law and democracy.

Wojciech Klicki
Vice-President
Panoptykon Foundation

Lori Roussey
Executive Director
Data Rights France

Eleftherios Chelioudakis
Executive Director Homo Digitalis

Anaïs Franquesa
Director, Irídia — Centre for the Defence of Human Rights

Malte Spitz
Secretary General
Gesellschaft für Freiheitsrechte e.V.

[redacted]