Written comment by Data Rights France, Homo Digitalis the Hungarian Civil Liberties Union and Irídia – Centre for the Defence of Human Rights as third parties intervening in the case Brejza v. Poland (App. Nos. 27830/23, 27632/23, 26531/23, 27840/23, 27942/23, 27998/23, 35514/23, 35791/23, 36474/23)

Dear Sir or Madam,

1. On behalf of Data Rights France, Homo Digitalis, the Hungarian Civil Liberties Union (HCLU), and Irídia – Centre for the Defence of Human Rights, we have the honour of transmitting to you our third-party intervention, as authorised by the decision notified on 12 February 2025.

2. In the following comments, the Interveners present some of the unique issues the use of spyware technology raises, as well as the legal and practical obstacles their organisations have faced representing clients before national institutions in cases involving the use of spyware. They would also like to present what conclusions may be drawn from their experiences.

I. The approach to be taken by the Court

3. The Interveners submit that, based on their experience with cases involving targeted surveillance, the Court should consider the following circumstances.

A. The strict application of the obligation to exhaust domestic remedies needs a nuanced approach in cases of targeted surveillance with spyware

4. Recognising the practical obstacles faced by potential victims of unlawful surveillance, the Court has developed a specialised test for assessing victim status in surveillance cases. In *Klass and Others v. Germany* (5029/71) and *Malone v. the United Kingdom* (8691/79), the Court has already established that, under certain conditions, applicants may claim to be victims of surveillance without proving that it has actually occurred, due to the inherent difficulties in substantiating such allegations.

5. Practical experience demonstrates that remedial institutions in surveillance cases are often ineffective, making the requirement to exhaust domestic remedies before seeking recourse from the Court an onerous, time-consuming, costly, and ultimately unnecessary burden for potential applicants (see Hungary and Spain §§ 25; 29). Even when a remedy appears effective, the government may simply eliminate it (see Greece § 23). In light of this reality, the Court should consider taking a pragmatic approach, as it did in assessing victim status, and adopt a more flexible stance on admissibility. If existing remedies can be shown to be ineffective *in abstracto*—simply by referring to the laws governing them—or if an applicant can reasonably demonstrate that a given remedy is ineffective in practice, the Court should not impose a strict exhaustion requirement.

B. Governments systematically breach Article 18 of the Convention

6. The Court astutely observed in *Weber and Saravia v. Germany* (54934/00) that "a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it" (§ 106). The prevalent misuse of the legitimate aims set out in Articles 8(2) and 10(2) of the Convention as a pretext for surveillance and the suppression of civic activism suggests that this issue is widespread and requires the Court's careful consideration. In the Interveners' jurisdictions, it is national security that can serve as a veil for state actions that facilitate repression rather than protect the common good. In Greece, Hungary, and Spain, authorities have systematically invoked national security to justify the surveillance of journalists, lawyers, activists, businesspersons, and political opponents.

C. Applying practical experience to some of the safeguards set out in the Roman Zakharov case

7. The Interveners submit that several safeguards established in *Roman Zakharov v. Russia* (47143/06), which form part of the "necessary in a democratic society" standard—considered under the "quality of law" requirement in surveillance cases—require updating to better reflect the realities of modern secret surveillance, particularly cases involving spyware.

i. Authorisation of interception

8. Spyware tools are highly intrusive, capable of granting access to all information stored on a person's electronic device, effectively providing a complete view of their private life, which needs to be taken into consideration when designing the authorisation process. It is crucial that the authorising judicial body be fully informed of the exact technical capabilities of the technology proposed to be deployed, and receive a well-reasoned authorisation request (see Hungary and Spain §§ 27; 29.1.; 31.2.). This request should clearly specify which capabilities will be used, for what purposes, and include a detailed assessment of necessity and proportionality. To ensure the effectiveness of the procedure, judges must have sufficient technical expertise. Merely requiring that surveillance measures be authorised by a judicial body, however, appears to be insufficient to prevent abuse. If judges oversee authorisations for extended periods, if there is little variation in the composition of authorising bodies, or if too few judges are assigned to this role, they may develop close collegial ties with the authorities they are meant to oversee. Additionally, they may become overly accustomed to their task, treating authorisation as a mere formality (see Hungary § 27). Under such circumstances, the judicial bodies' safeguard function is effectively undermined, as reflected in Chapter IX of the Venice Commission's *Report on the Democratic Oversight of the Security Services* [CDL-AD(2015)010]. For these reasons, the Court should consider establishing

further requirements regarding judicial bodies. It is crucial that the authorising body be fully informed of the exact technical capabilities of the technology being deployed and receive a well-reasoned authorisation request (see Hungary and Spain §§ 27; 31.2.). This request should clearly specify which capabilities will be used, for what purposes, and include a detailed assessment of necessity and proportionality. To ensure the effectiveness of the procedure, judges must have sufficient technical expertise.

ii. Supervision

9. Spyware's extremely intrusive nature affects the framework of supervision too. To prevent abuse, every instance of access and data retrieval must be meticulously logged, ensuring that a judicial supervisory authority has full oversight of all information accessed or obtained by the deployer of the technology. Supervision must be continuous, and any data not strictly necessary for the specific operation must be promptly discarded.

10. At the outset of an operation, it may be necessary to use the technology to access a broader range of data on a device to identify the specific communications or information of interest. However, as the operation progresses, the scope of intrusion should be progressively narrowed—within defined time periods—and once all necessary information has been obtained, surveillance should continue without the use of spyware. Consequently, there must be a strictly controlled and continuous reduction in the intrusiveness of the measures over time, with regular oversight by the supervisory authority to ensure compliance. It is of paramount importance, however, that the supervisory authority have the necessary technical knowledge to effectively carry out its tasks.

ii. Effective remedial measures

11. Where individuals have the right to request disclosure of whether intelligence services hold data on them, those services may be permitted to issue a standard response refusing to confirm or deny data processing in order to protect their databases (see Hungary § 25.2.). While the objective of this approach is legitimate, its automatic and indiscriminate application, without assessing the individual circumstances of data subjects, is not. Sensitive databases can still be safeguarded if a proportion of data requests are granted, provided that the pattern of responses does not reveal intelligence operations. Clear protocols should be established to allow for the selective disclosure of information without compromising national security, with a particular focus on prioritising transparency in cases of potential abuse. Courts must have the authority to override automatic denials, especially when they serve as a pretext for concealing fundamental rights violations, and most importantly where a State fails to implement post-factum notification.

iii. Informational redress as just satisfaction

12. Although the Court has extensive case law on what constitutes an effective remedial institution, it should also consider what form of redress can provide just satisfaction for victims of targeted surveillance. The primary objective of most victims is to uncover what information has been unlawfully collected about them and who it was shared with, as spyware enables the operator to access their most sensitive data going back for years. The harm can be especially grave in the case of journalists or lawyers, where journalistic sources or lawyer-client privileges may be compromised. Since the collected data are almost always classified, a prominently appropriate form of compensation would be the declassification and disclosure of the data lifecycle since collection, together with accompanying surveillance material. To ensure meaningful redress, the Court should require that, during remedial proceedings, the competent judicial body has the authority to assess not only the formal legality of the classification process but also the substantive legality of the data handling itself. Furthermore, it should have the power to declassify and disclose any unlawfully obtained data to the individual concerned—at least those that do not compromise ongoing operations, and, within a reasonable and foreseeable timeframe, all remaining data (see Hungary and Spain §§ 26; 30). Notably, the potential declassification and disclosure of intelligence data serve as a deterrent against the unlawful use of surveillance powers, providing an essential safeguard against abuse.

II. Spyware may cause more serious harm than mere surveillance

A. Hacking as a disproportionate technique, beyond the notion of surveillance

13. The appreciation of what is proportionate in European law has evolved. Although Article 10(2) of the Convention grants states a margin of appreciation where freedom of expression is concerned, this margin is not offering States unlimited powers. In fact, doctrine[1] has pointed out that this paragraph must be interpreted with being in line with the provision of effective protection. That is, that the overriding role of the Convention is to effectively protect human rights in Europe. Besides, Article 17 of the Convention sets a strong safeguard for Europeans. As per the convention, "any act aimed at the destruction of any of the rights and freedoms" is prohibited.

14. As a result, the provisions of the Convention must be interpreted restrictively where the defense of national sovereignty or similar legal exemptions may be invoked by a State. This echoes the spirit of Article 11 of Convention 108. Moreover, an assessment by a State of what may be appropriate and proportionate must be done in a democratic fashion[2].

---

[1] Van Dijk and Van Hoof – *Theory and Practice of the European Convention on Human Rights*, Kluwer, 1998, p. 74.
[2] R. Clayton, H. Tomlinson – *The Law of Human Rights*, Oxford, 2000, p. 285.

15. Beyond the assessment of whether legal exemptions granted to States were abused, it is worth analysing facts through proportionality balancing tests. The three factors being that legal measures are expressly found in the law (*Malone v. The United Kingdom* (8691/79) and *Sunday Times v. The United Kingdom* (6538/74)), the aim served is legitimate and is truly necessary in a democratic society (*Handyside v. the United Kingdom* (5493/72)).

16. In the Brejza case, the Pegasus hacking tool enabled law enforcement to access *inter alia* 10 years of communications of Mr Brejza. Access to such considerable amount of data would probably not have been possible through a mere real-time interception tool. Applying the proportionality balancing exercise only goes to confirm that such access could not be proportionate. Indeed, as developed by the Applicants, the ability to deploy such a potent technique the way it was deployed was not provided for in Polish law. With regards to the legitimacy and necessity of the deployment of Pegasus on the Applicants, given the apparent political motives these two conditions too are not met.

17. What is more, the treatment of extracted data after extraction illustrates the disproportion of Polish law enforcement actions. Indeed, data extracted was later reorganised and sometimes merged to build a new narrative. Such actions by authorities are akin to digital sabotage of target citizens. The tampering with data was probably not done directly on the phones, to not raise the suspicions of victims. It must nonetheless be stressed that tampering directly with the primary source of data, i.e. here targets' phones, is made possible by powerful hacking tools like Pegasus. *This is a core stake of hacking by States*. Indeed in India, reports on human rights defenders and activists have documented they were hacked by Pegasus and then infected with malware that enabled to plant incriminating evidence on their computers to ensure their jail convictions[3]. The Indian case illustrates that hacking tools are able to and/or facilitate the modification, removal or addition of data to tamper with evidence. In other words, this Indian case illustrates how hacking tools are beyond mere surveillance tools. Especially as the facts of the Indian case date back to 2018. Companies selling tools like Pegasus sell the ability to gain complete control over a device. The more powerful the hacking tool, the higher its market share. Hacking tools enabling one to gain complete power over one's phone or computer are unacceptable in democratic societies as they can put political dissidents and human rights defenders at the mercy of the arbitrariness of leaders. In particular today, when citizens' communications and critical public infrastructures rely on data integrity.

---

[3] See for instance Sawhney, R. S., Chima R. J. S., In India, malware plants false "evidence" of crime on activist's laptop, Access Now, 2023. Accessible online: <https://www.accessnow.org/india-malware/> (accessed on February 22, 2025) and Greenberg, A., Police Linked to Hacking Campaign to Frame Indian Activists, Wired, 2022. Accessible online: <https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/>

B. Right to respect for private and family life

18. With regards to Article 8 of the Convention, to not repeat what the Applicants already shared with this court the interveners shall simply point out relevant safeguards in the Convention 108+ on the protection of individuals with regard to the processing of personal data safeguards. In the Brejza case as well as the ones we support throughout Europe we observe that legal exemptions like national security and the fight against corruption are evoked to target human right defenders and journalists.

19. For this reason we hope to be of service to the Court by pointing out that Article 11 of Convention 108+ expressly provides that no exceptions to its chapter on basic data protection principles may be made when a State evokes exceptions pertaining to the "protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest". Unless such exceptions are provided by law (i), respect the essence of rights and freedoms (ii) and are necessary and proportionate (iii). These conditions are cumulative.

20. In practice the deployment of Pegasus on the Applicants was found by Poland itself as having violated its law (i), leads to egregious violations of individuals' right to freedom of expression and the right to a private and family life (ii), and was neither necessary nor proportionate (iii)—see below for more details on proportionality specifically. This observation is shared with regards to the cases respectively supported by Irídia and the Hungarian Civil Liberties Union. As a consequence, even when evoking legal exemptions, States should uphold the most basic data protection principles, such as the principles of legitimacy, transparency and security.

21. Hacking spyware poses a substantial threat to the rule of law. That being said, additional abuses are currently associated with spyware use in Europe and deserve to be drawn to the attention of this court.

III. Challenges victims of spyware face in the Interveners' countries

22. The Interveners—all of whom come from States examined by the PEGA Committee of the European Union after spyware scandals—allege that their experiences are symptomatic of broader tendencies regarding the dysfunction of legal institutions meant to protect fundamental rights in the context of spyware and secret surveillance.

i. Greece

23. Lack of effective remedies: 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. 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.

24. National security used as a pretext: According to Resolution 2513 (2023) of the Council of Europe "in Greece, it has been confirmed that a member of the European Parliament and a journalist have been wiretapped by the intelligence agency and targeted with Predator spyware, and media reports revealed further possible targets of Predator, including other high-profile politicians. Spyware appears to have been used on an ad hoc basis for political and financial gains" (5.2). The use of spyware was justified with national security in all instances.

ii. Hungary

25. Lack of effective remedies: In the cases of the seven clients targeted with Pegasus spyware and represented by the HCLU, Hungarian remedial institutions have proven incapable of providing any redress. This is because (1) all non-judicial avenues are ineffective, as established by the Court in *Szabó and Vissy v. Hungary* (37138/14) and *Hüttl v. Hungary* (58032/16); (2) redress cannot be obtained through the courts; and (3) there is a lack of effective remedies, as required by the Court's case law. In particular:

25.1. The ministerial complaint, the complaint to Parliament's National Security Committee, the Fundamental Rights Commissioner's investigation and the procedures of the National Authority for Data Protection and Freedom of Information (hereinafter: DPA) are ineffective, as set out in §§ 83; 82; 84–85 of *Szabó and Vissy* and § 18 of *Hüttl*, respectively.

25.2. There is no requirement to notify individuals subjected to interception, and the courts' jurisdiction is contingent on the interception subject's ability to prove that their communications have been monitored. In practice, potential victims must: (1) Submit an access request to the intelligence services, requesting disclosure of whether their data has been processed and the relevant case file number. (2) Face an automatic denial, as intelligence services refuse to disclose such information on the grounds that even confirming or denying the

request would compromise their databases. (3) Initiate a lawsuit to obtain the requested information—a process that typically takes around two years. (4) If successful in court, they receive only the case file number of a classified document, for which they may request security clearance. (5) Be denied clearance in practice, as authorities systematically reject such requests.

26. Impossibility of declassification in cases of illegal surveillance: Declassification of surveillance material on the grounds that they were collected unlawfully is presently not possible under Hungarian law, as classification supervision carried out by the DPA only concerns the legality of the classification itself, which in turn is a separate procedure from, and is not necessarily affected by the legality of the collection of data.

27. Deficiencies in judicial authorisation: A freedom of information request (FOI) submitted by a Hungarian Member of Parliament revealed that between 2010 and 2021, judges approved every request for secret surveillance on national security grounds in cases where judicial authorisation was required. Additionally, a FOI request filed by the HCLU revealed that authorising bodies are not informed about the specific technologies used for secret surveillance during the authorisation process, preventing them from properly assessing the level of intrusiveness.

28. National security used as a pretext: According to Resolution 2513 (2023) of the Council of Europe "in Poland and Hungary, Pegasus surveillance spyware has been illegally deployed for political purposes to spy on journalists, opposition politicians, lawyers, prosecutors and civil society actors, apparently as part of a system or an integrated strategy" (5.1). In Hungary, national security was invoked in every single procedure that the HCLU initiated with its clients.

iii. Spain

29. Lack of effective remedies: In the Spanish context, the fight against state-sponsored espionage is primarily conducted through the criminal justice system, since the actions of the government through the intelligence services may be criminal in nature. In practice, however, the judicial route has failed for a number of reasons:

29.1. **Lack of technical expertise:** Judges and courts lack sufficient technical knowledge to understand the scope, capabilities and implications of spyware.

29.2. **Obstruction of justice:** Although a specialised cybercrime prosecutor's office exists, it does not actively defend citizens' rights or promote legal action. Instead, it hinders coordinated investigations between different judicial bodies, leaves prosecutions to private or popular prosecutors, and prevents the sharing of investigation results.

29.3. **Restrictions on the investigation of senior officials:** The Official Secrets Act prevents current or former CNI directors from fully answering questions

during interviews with investigators or involved parties. In addition, the former director of the CNI claimed in an official statement to a court that she was unable to speak freely because of the existence of the law. In any case, there would be no authorisation to make personal statements by those responsible for the CNI at the time of the intervention.

29.4. The **Ombudsman** (Defensor del Pueblo) is involved in cases of state espionage when it is the only constitutional body with access to classified information and can question the work of the CNI. However, the Law on Official Secrets prevents it from commenting on the content of this information, highlighting the lack of effective means to investigate these cases and protect the human rights that have been violated. (The Court has already ruled in *Hüttl v. Hungary* that a failure to access all intelligence material renders a remedy ineffective; see Hungary § 25.1.) Although in several cases victims of surveillance have asked the body for information in order to support their legal case, the Ombudsman stated that he did not have any information on the matter.

30. Impossibility of declassification in cases of illegal surveillance: Declassification is the only way to access classified information. In theory, an examining judge can request declassification for specific documents, information, or authorisations. However, in practice, this procedure is rarely used due to the absence of clear criteria for declassifying information. While judges can submit requests, approvals are rare, making declassification a purely political decision. Although a "contentious-administrative appeal" may be lodged with the Supreme Court if a declassification request is denied, this procedure only concerns the formal legality of the classification process, and not whether the classified data is being held legally. Disclosure is heavily restricted, and even when technical evidence confirms spyware infections, the only information released may be whether the National Intelligence Centre (CNI) acknowledges surveillance—without clarifying its scope, use, or limitations regarding Pegasus.

31. Deficiencies in judicial authorisation: The weakness of the Spanish legal framework regarding the intelligence functions of the CNI and its control is a major obstacle to effective remedies in cases currently before domestic courts. The legal framework in Spain presents certain challenges that facilitate interception without effective oversight and hamper subsequent investigations. Although there are rules governing the interception of communications, they do not always ensure adequate oversight, either before or after the interception, and do not meet the standards of clarity, predictability, accessibility and protection of individual rights. In particular:

31.1. The CNI, established by **Law 11/2002**, provides intelligence to protect Spain's security, territorial integrity, and institutions. While authorised to conduct "security investigations," the law lacks specifics on their scope or limits.

Parliamentary oversight is restricted to the Official Secrets Commission, which monitors classified funds but limits MPs' access to certain information. This commission has access to classified information, but with restrictions. In other words, it defines a type of information to which MEPs do not have access under any circumstances.

31.2. **Organic Law 2/2002** establishes judicial oversight of the CNI, requiring a Supreme Court judge's authorisation for measures affecting home inviolability and communication secrecy. The law contains only one article that mentions the obligation of judicial authorisation, without defining its scope, the limits of its duration (with the possibility of its extension indefinitely after the first three months) and the control and follow-up during and after the first three months. Therefore, with the limited information available, it is not possible to assess the compliance with the principles of legality, necessity and proportionality of the de facto measures taken by the CNI against the spied upon persons.

31.3. Decisions authorising fundamental rights violations are classified under **Law 9/1968, Official Secrets Act**, limiting transparency. Judges can request declassification, but access remains partial and unverifiable. Financial oversight falls to a confidential congressional committee, which met only once during the XIV legislature when the espionage operation was exposed.

32. Most of the CNI's work is kept secret and inaccessible, with no mechanism for transparency or access. In this last respect, the absence of clarity and definition in the regulatory framework governing the CNI hinders the delineation of the scope and modalities of the exercise of the discretionary powers conferred upon the authorities. This impedes the ability to ensure the provision of the minimum level of protection that individuals are entitled to in a democratic society governed by the rule of law, as stipulated by the standards of international human rights law.

33. **We appreciate the opportunity to submit these comments to the Court and hope they prove useful.**

26 February 2025.

Yours faithfully,

Lori Roussey,
Executive Director,
Data Rights France

Máté Szabó,
Director of Programs,
Hungarian Civil Liberties Union

Eleftherios Chelioudakis,
Executive Director
Homo Digitalis

Anaïs Franquesa Griso,
Executive Director,
Irídia, Center for Human Rights