

**Hungary, F?városi Törvényszék (Metropolitan Court of Budapest),  
105.K.701.218/2023/16 (Pegasus case), first instance, 8 February  
2024**

Member State

 Hungary

---

Topic

Rule of Law

---

Sector

Predictive Justice

---

Deciding Court Original Language

F?városi Törvényszék

---

Deciding Court English translation

Metropolitan Court of Budapest

---

Registration N

105.K.701.218/2023/16

---

Date Decision

8 February 2024

---

ECLI (if available)

N/A

---

National Follow Up Of (when relevant)

N/A

---

EU legal sources and CJEU jurisprudence

N/A

---

ECtHR Jurisprudence

N/A

---

## Subject Matter

Secret surveillance, Data Protection Authority (DPA), ensuring the data subject's rights, classified data and descriptive elements, request for access to classified data, obligation to provide reasoning

---

## Legal issue(s)

The plaintiff is a journalist who, based on the examination of their mobile phone, believed that their device had been unlawfully surveilled using the Pegasus spyware. The plaintiff turned to the Data Protection Authority (DPA), which rejected the plaintiff's request without substantive reasoning and ensured the exercise of their rights only in a formal manner.

---

## Request for expedited/PPU procedures

NO

---

## Interim Relief

N/A

---

## National Law Sources

Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Data Protection Act)

---

## Facts of the case

The plaintiff is a journalist who, based on the examination of their mobile phone, believed that their device had been unlawfully surveilled using the Pegasus spyware.

The plaintiff initiated a procedure before the Data Protection Authority (DPA), alleging violations of personal data processing laws and seeking the protection of their rights.

The DPA investigated whether any of the data controllers authorized to conduct covert information gathering had, or currently has, processed the plaintiff's data using the Pegasus spyware. As part of its inquiry, the DPA contacted the National Security Service for data verification, and reviewed the relevant sections of the minutes from closed sessions of the National Security Committee of Parliament concerning the complaints submitted by the plaintiff. The investigation concluded that no illegality regarding the processing of the plaintiff's data had been identified

In light of the findings, the DPA concluded in its decision that no violation of personal data processing regulations had occurred, and it rejected the plaintiff's request on this matter. The DPA ensured the plaintiff's rights by providing information on the completion of all necessary verifications.

The DPA's decision included the designation of "classified information" in four places; the plaintiff was not granted access to the unredacted version of the decision.

The plaintiff requested a judicial review of the decision.

---

## Reasoning (role of the Charter or other EU, ECHR related legal basis)

The court stated that the exercise of the data subject's rights related to classified data can be realized through the DPA and the courts. In this process, the DPA must fulfill a substantive fundamental rights protection function, and its procedure cannot result in the mere formal enforcement of rights.

The court found that the DPA violated its fundamental rights protection function by failing to

include the descriptive elements of the classified data (e.g. classification level, basis for classification, classifying authority, duration of classification, access authorization level) in the redacted decision. These elements would have enabled the plaintiff to submit a request for access. The disclosure of descriptive elements does not imply that the plaintiff is necessarily the subject of surveillance, as such information can only be contained in the classified data itself, which is clearly distinct from the descriptive elements.

Furthermore, the court determined that the DPA did not fulfill its obligation to provide adequate reasoning. The Data Protection Act allows that, if the data subject's rights are lawfully restricted by law, the DPA must ensure those rights in a manner that does not undermine the interests underlying the restriction (e.g. national security interests). However, according to the court, this cannot lead to the hollowing out of rights. To fulfill its fundamental rights protection function, the DPA must provide reasoning - sufficient to satisfy a fundamental rights balancing - regarding the relationship between the method and timing of ensuring the data subject's rights and the national security interests. This requirement applies even when the DPA cannot disclose to the plaintiff whether they were subject to surveillance.

For these reasons, the court annulled the DPA's decision and ordered the DPA to conduct a new procedure.

---

Relation of the case to the EU Charter

N/A

---

Relation between the EU Charter and ECHR

N/A

---

Use of Judicial Interaction technique(s)

N/A

---

Horizontal Judicial Interaction patterns (Internal – with other national courts, and external – with foreign courts)

N/A

---

Vertical Judicial Interaction patterns (Internal – with other superior national courts, and external – with European supranational courts)

N/A

---

Strategic use of judicial interaction technique (purpose aimed by the national court)

N/A

---

Impact on Legislation / Policy

N/A

---

Notes on the national implementation of the preliminary ruling by the referring court

N/A

---

Connected national caselaw / templates

N/A

---

(Link to) full text

N/A

---

Author

Bernadette Somody, Eötvös Loránd University (ELTE)

---