Funded by the European Union

Strategic Litigation for Rights in Europe: Building Knowledge, Skills and Connections for Legal Practitioners to Use the EU Charter of Fundamental Rights
(STARLIGHT)

LEGAL CLINIC ARGUMENTS

RULE OF LAW AND CIVIC SPACE

Zuzanna Nowicka, Sònia Olivella Saludes, Michaël Merrigan, Anna Maria Katsimeni, Daniela Constantin, Pavel Koniar, Anna Białek

Hertie School
Executive Education

HUNGARIAN HELSINKI COMMITTEE

Imprint

Hertie School Executive Education in collaboration with the Hungarian Helsinki Committee

Text
Zuzanna Nowicka
Sònia Olivella Saludes
Michaël Merrigan
Anna Maria Katsimeni
Daniela Constantin
Pavel Koniar
Anna Białek

Mentor
Lázsló Detre

Edited by
Kersty McCourt

Publisher
2024 STARLIGHT

The STARLIGHT programme is funded by The Citizens, Equality, Rights and Value programme (CERV) of the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the EU CERV-Programme. Neither the European Union nor the granting authority can be held responsible for them.

Funded by the European Union

hertie-school.org/en/customised/starlight

The Legal Clinics are a core part of the STARLIGHT programme, where all participants worked in groups to develop legal arguments on a real or potential case. Groups were mentored by their course leads and one case per thematic stream selected for publication.[1]

LEGAL ARGUMENTS

CASE – NATURE OF THE PROBLEM

In Spain, beginning from May 2020 the mobile phone of a criminal lawyer (Mr. X) was infected with Pegasus spyware. He was defending political representatives and civil society leaders in a relevant criminal proceeding and coordinating the legal strategy before both national and international courts. This infection compromised his privacy, secrecy of communications and, of course, professional secrecy. Under Spanish law, the use of surveillance measures might be authorized only in relation to threats to national security and the prevention and investigation of serious crimes. However, Mr. X wasn't being investigated in relation to any criminal proceedings.

This case is a part of a broader pattern of political espionage, organized by state government agencies, targeting a wide range of politically relevant actors. At least, 65 people (including specially protected victims such as elected political representatives, MEPs, journalists or lawyers) have been targeted by spyware technologies such as Pegasus.

In May 2022, Mr. X submitted a criminal claim against the NSO Group - a private entity that owns Pegasus - and the Spanish National Intelligence Centre (CNI) for acts of espionage, interception of communications, illegal intrusion into computer devices and acquisition and production of precursors to espionage. The surveillance was allegedly conducted by the CNI, a government body using Pegasus. The criminal court recently issued a resolution dismissing the procedure, without having carried out the minimum investigation. The State declined to provide any information to Mr. X as to whether he was being, or had been surveilled.

The only government body competent to use surveillance tools such as Pegasus is the CNI, governed by Organic Laws 11/2002 and 2/2002. To conduct surveillance, the CNI must request authorization from a competent magistrate of the Supreme Court. Spanish law does not oblige the CNI to inform individuals about surveillance measures being used against them.

Moreover, internal conditions for the processing, use, storage, and communication of the data obtained through surveillance is classified.

[1] The final legal arguments have been lightly edited but are the work of the group. Experimental legal arguments were encouraged. Readers are encouraged to draw inspiration from the work but should note that there may be some legal inaccuracies.

Funded by the European Union

LEGAL ANALYSIS

1. Legal basis – EU law

a. National security claim

The preliminary question in this case is whether it falls within the scope of EU law. Under the EU framework, national security remains the sole responsibility of each Member State (Article 4(2) TEU). However, according to the Court of Justice of the European Union's (CJEU) case law, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member State from their obligation to comply with that law (joined cases C-511/18, C-512/18, and C-520/18, paragraph 99). In its judgments, the CJEU examines whether the measure a state has adopted for national security, actually serves that purpose. In case C-33/22, the CJEU judged that proceedings intended to exercise political scrutiny did not constitute activity intended to safeguard national security. By analogy, it seems that in cases of unfounded use of surveillance measures, the national security claim can also be dismissed.

b. Potential breach of Article 8 of the LED - unlawful data processing

During the alleged surveillance using the Pegasus system provided by the NSO group the CNI, a government body, processed the personal information of Mr. X. The use of personal data by criminal law enforcement authorities is governed by the Law Enforcement Directive (EU) 2016/680 (LED). The LED was implemented by Spain by adopting Organic Law 7/2021.

According to Article 8(1) of the LED, the processing of personal data can be considered lawful only if, and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

According to Organic Law 11/2002 the CNI has to conduct its actions, including surveillance and other intelligence operations to meet specific purposes, for example to prevent threats to national security. The preliminary issue with this regulation is that it's too vague (see the Charter section). At the same time even with such a broad basis for the use of surveillance, the use of Pegasus by the CNI against Mr. X appears to be unfounded. It seems that it was purely politically motivated, as he was not being investigated in relation to any criminal proceedings. Therefore, the processing of his personal data by the CNI in connection with the Pegasus surveillance cannot be considered lawful.

c. Potential breach of Article 14 of the LED - refusal of the access to information about processing of personal data

The State has not provided Mr. X any information about the processing of his personal data in relation to the use of surveillance against him. This practice potentially breaches the LED. According to Article 14 of the LED, individuals have the right to obtain confirmation from the relevant authorities as to whether or not their personal data are being processed. This includes information about the purpose and legal basis

for the processing, such as surveillance. If the relevant authority denies access to this information, for example to avoid prejudicing the investigation of a criminal offense, it must provide reasons for the refusal. This was not the case for Mr. X.

d. Potential breach of Article 54 of the LED - absence of judicial remedy

Spanish law doesn't explicitly provide a clear, accessible and effective judicial remedy for individuals who have discovered they were subject to surveillance. Mr. X unsuccessfully tried to challenge the surveillance (and the related processing of his personal data) by submitting a criminal claim against the NSO Group. The procedure was minimal; the court dismissed the case without thoroughly examining the merits of his claims or even confirming the surveillance, let alone providing justification for it.

This is a potential breach of Article 54 of the LED which states that Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed.

The lack of effective judicial remedy in this case is especially problematic because it seems that the use of surveillance measures, and therefore the data processing, was unfounded and thereby unlawful, as explained above.

Moreover, the limited oversight of the CNI concerning the use of surveillance measures is not sufficient to prevent potential breaches of the rights of individuals.

e. Incorrect transposition of the LED

Article 2.3(d) of the Organic Law explicitly states that it doesn't apply to data processing governed by regulations on classified matters, including those related to national defense. This means that the activities of the CNI, which are classified according to Article 5(1) of the Organic Law 11/2002 fall outside of the scope of the law implementing the LED. This possibly amounts to an incorrect transposition of the directive.

2. Legal basis – Charter

Spanish laws governing the processing of personal data in relation to surveillance are governed by the law implementing the LED. Consequently, they fall within the scope of EU law. According to Article 51(1) of the Charter of Fundamental Rights, the provisions of the Charter are addressed to Member States when they are implementing Union law. Therefore, the Charter is applicable in the case of Mr. X.

According to Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognized by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may only be made if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. According to Article 53 of the Charter, the level of protection granted by the Charter cannot be lower than the level of protection granted by the European Convention of Human Rights (ECHR). In the context of Article8 of the ECHR, which guarantees the right to privacy, the European Court

of Human Rights (ECtHR) stated that legal provisions governing interception of communications need to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures need to be defined with sufficient clarity. Provisions on the discontinuation of secret surveillance measures need to provide sufficient guarantees against arbitrary interference. Domestic law should be clear as to the circumstances in which intercepted material will be stored and destroyed. The authorization procedures should ensure that secret surveillance measures are ordered only when "*necessary in a democratic society*." Adequate supervision of interception should be guaranteed, and effective remedies should be provided e.g., some form of notification or adequate access to documents relating to interceptions (Zakharov v. Russia, application no. 14881/03, paragraph 302; see also Pietrzak et Bychawska-Siniarska and others v. Poland, nos. 72038/17 and 25237/18).

In the case of Mr. X, the limitation of his right to privacy (Article 7 of the Charter) and the protection of personal data (Article 8 of the Charter) was not provided by "*accessible and foreseeable law*." According to longstanding ECtHR case law, the condition that a limitation of a right must be prescribed by law and requires not only that the impugned measure has a legal basis in domestic law, but also that the quality of the law in question is such that it is accessible to the person concerned and foreseeable as to its effects (see, among others, Sindicatul "Păstorul cel Bun" v. Romania [GC], no. 2330/09) § 153). The Spanish law governing the use of surveillance measures by the CNI is very vague regarding the circumstances in which they can be used and does not clearly define the categories of individuals whose data can be intercepted. This vagueness undermines the requirement that any limitation on rights must be provided by law in a clear and predictable manner.

Moreover, the internal regulations governing the use of personal data by the CNI are not accessible to the public, further compromising the principle of legality.

Even if the limitations were considered provided by law, it is disproportionate and unnecessary. According to longstanding case law of the CJEU, legislation that permits public authorities to have generalized access to personal data must be regarded as compromising the essence of the fundamental right to respect for private life and the protection of personal data (case C-362/14, paragraph 94). The surveillance of Mr. X, conducted without any connection to criminal proceedings, cannot be considered necessary to protect national security.

Additionally, Mr. X was not granted an effective judicial remedy (Article 47 of the Charter) regarding the processing of his personal data in relation to the surveillance. The court dismissed the case without thoroughly examining the merits of his claims or even confirming the surveillance, let alone providing justification for it. The issue is more structural in nature because, even though one can challenge the decision to use surveillance in court, the Spanish law governing the CNI does not explicitly provide a clear and effective judicial remedy regarding the processing of personal data in relation to surveillance. According to Article 54 of the LED, Member States must provide for the right of a data subject to an effective judicial remedy where their rights under the Directive have been infringed.

Funded by the European Union

CONCLUSION AND RECOMMENDATIONS

Spanish law is too vague and broad regarding the cases in which the use of surveillance measures are permissible. Therefore, it seems that in many cases both the use of surveillance and the related processing of personal data should be considered unlawful. This constitutes a potential breach of Article 8 of the LED and Article 7 and 8 of the Charter.

Moreover, using unlawful surveillance measures against individuals while denying them the right to confirm the processing of their personal data and access information on the purposes and legal basis for such processing, constitutes a violation of Article 16(1) TFEU (which grants all individuals the right to the protection of their personal data), in conjunction with Article 2 TEU (which outline the founding values of the EU), Article 14 of the LED, and Articles 7 and 8 of the Charter. Additionally, the lack of transparent and effective oversight of the CNI's surveillance activities infringes these same provisions.

Subsequently, not providing individuals who have been denied such information an effective judicial remedy constitutes a violation of Article 54 of the LED and Article 47 of the Charter.

Finally, Spain may have incorrectly transposed the Law Enforcement Directive (LED). The law implementing the directive does not apply to data processing governed by regulations on classified matters. However, the LED does not provide for such an exception. If the data is being processed for the purposes outlined in Article 1(1) – as at least some of the data processed by the CNI is – it falls within the scope of the LED regardless of whether the data is classified.

Consequently, as there is no clear and effective possible judicial remedy under the Spanish law, the European Commission should initiate infringement proceedings based on the above legal arguments, in particular breaches of the LED and associated Charter rights.

Alternatively, if a national procedure is launched, we recommend for the judge to make a request for a preliminary reference based on the following questions:

- Should Article 16(1) of the TFEU, in conjunction with Article 2 of the TEU, Article 8 of the Charter, and Article 2(a) of the LED, be understood as precluding the national law that allows for surveillance and subsequent data processing, solely on the basis that it must be formally justified by a need to protect national security, including preventing and averting threats such as terrorism, espionage, organized crime, and other activities that could harm a Member State's national interests?
- Should Article 16(1) of the TFEU in conjunction with Article 2 of the TEU, Article 8 of the Charter and Article 4(1)(a) of the LED be understood as precluding rules that automatically classify the processing, use, storage, and communication of the data obtained through surveillance and other intelligence operations?

Funded by the European Union