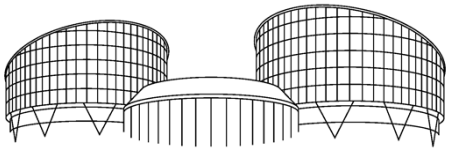

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIRST SECTION

CASE OF KLAUDIA CSIKÓS v. HUNGARY

(Application no. 31091/16)

JUDGMENT

Art 8 and Art 10 • Private life • Correspondence • Freedom of expression • Lack of adequate procedural safeguards for a journalist to challenge the alleged use of secret surveillance with a view to revealing her sources

Prepared by the Registry. Does not bind the Court.

STRASBOURG

28 November 2024

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Klaudia Csikós v. Hungary,

The European Court of Human Rights (First Section), sitting as a Chamber composed of:

Marko Bošnjak*, President*,
Alena Poláčková,
Péter Paczolay,
Erik Wennerström,
Raffaele Sabato,
Lorraine Schembri Orland,
Ioannis Ktistakis*, judges*,
and Ilse Freiwirth, *Section Registrar,*

Having regard to:

the application (no. 31091/16) against Hungary lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Hungarian national, Ms Klaudia Csikós ("the applicant"), on 17 May 2016;

the decision to give notice of the application to the Hungarian Government ("the Government");

the parties' observations;

Having deliberated in private on 13 February and 5 November 2024,

Delivers the following judgment, which was adopted on that last-mentioned date:

INTRODUCTION

1. The application concerns the alleged tapping of the applicant's telephone calls with a close acquaintance, apparently with the view of revealing her journalistic sources. It raises issues under Articles 8 and 10 of the Convention.

THE FACTS

2. The applicant was born in 1975 and lives in Budapest. She was represented before the Court by Mr A. Cech, a lawyer practising in Budapest.

3. The Government were represented by their Agent, Mr Z. Tallódi, of the Ministry of Justice.

4. The facts of the case may be summarised as follows.

5. The applicant is a journalist at *Blikk,* a daily paper.

6. In the applicant's submission, her phone has been tapped between 3 and 6 November 2015 by the investigation authorities with the view of identifying her journalistic sources.

7. On 6 November 2015 the Buda Central District Court authorised secret information-gathering measures against a police officer, T., including the tapping and recording of his telephone communications. The warrant,

justified in the context of an ongoing investigation into charges of active bribery and aiding and abetting abuse of authority (under Article 293(1)-(2) and Article 305(c) of the Criminal Code), was valid until 3 February 2016.

8. On 17 November 2015 the applicant received two telephone calls from T., a close acquaintance. Their conversations concerning a high-profile murder case were recorded. The transcripts of the recordings omitted the personal parts of the conversations not relevant to the ongoing criminal proceedings.

9. On the same day, the applicant published an article about the murder case on an Internet news portal. The following day she expanded the article.

10. On 15 December 2015 criminal proceedings were initiated against T. on charges of abuse of authority for having shared secret information with the applicant. The information gathered by way of the phone tapping was allowed to be used in evidence in those proceedings by a decision of the Budapest Regional Court of 4 January 2016.

11. The applicant lodged a criminal complaint against the Pest County Police Department. She reported her suspicion that her telephone call lists might have been unlawfully acquired. She submitted that her contacts in the police had been removed from their posts, which she alleged must have been because they had been identified as her sources of information. The investigating authority characterised her complaint as an allegation of abuse of power, under Article 305 of the Criminal Code. The applicant's criminal complaint was dismissed on 1 February 2016; the decision pointed out that call lists could be legitimately requested in ongoing investigations. The applicant complained against the decision, arguing that the transfer of her contacts in the police from their posts was evidence that her sources had been revealed through the monitoring of her calls. That complaint was also dismissed.

12. In the applicant's submission, she found out on 11 May 2016 in the context of the criminal investigations in respect of T. that her phone had been tapped so as to identify her sources in the police. She submitted that the phone used by her, which had been provided by her employer, had been tapped between 3 and 6 November 2015.

13. On 19 May 2016 the applicant lodged a complaint with the National Defence Service (*Nemzeti Védelmi Szolgálat*) on the basis of section 92(2) of the Police Act, seeking an investigation and redress in respect of the tapping of her phone and the acquisition of her call list. The applicant's lawyer maintained that he had plausible grounds to believe that in the second half of 2015, on the instruction of the National Defence Service, the Directorate of the National Security Service (*Nemzetbiztonsági Szakszolgálat*) had conducted a secret investigation in respect of the applicant, under the code name "German 8", concerning alleged offences of bribery and aiding and abetting abuse of authority. Furthermore, her call list had been accessed by the National Security Service in order to identify her sources. In the

applicant's understanding, both measures had been taken in accordance with section 72(1) of the Police Act, which allowed for the use of special measures without judicial authorisation in urgent cases and for a limited period of time. However, the secret surveillance measure had not been subsequently approved by a judge, as required by law, her data had not been deleted and she had not been questioned, either as a witness or as a suspect in the case. The applicant argued that the measures had had a deterrent effect on her work as a journalist and constituted a violation of her rights under Articles 8 and 10 of the Convention.

14. The National Defence Service rejected the complaint on 22 June 2016 as partly incompatible *ratione materiae* with the Police Act, since secret information gathering could not be challenged under that Act. The applicant was also informed that the conduct of the National Defence Service had otherwise been in accordance with the law; however, no further information could be provided since the complaint concerned ongoing criminal proceedings.

15. On 23 May 2016 the applicant lodged a similar complaint with the Minister of the Interior under section 11(5) of Act no. CXXV of 1995 on the National Security Services ("the National Security Act" – see paragraph 24 below). In his reply of 13 June 2016, the Minister offered general considerations on the lawful functioning of the services complained about. The Minister did not address the circumstances of the applicant's case but stated that the conduct of the National Security Service had been in compliance with the law. As regards the actions of the National Defence Service, the Minister explained that since it could not be challenged under the National Security Act, he examined the applicant's complaint under the Act on public interest disclosures. He stated in general terms that the conduct of the National Defence Service had complied with the law. However, no further information could be provided, as it related to ongoing criminal proceedings.

16. The applicant lodged a subsequent complaint with the National Security Committee of Parliament under section 14(4)(c) of the National Security Act, adding to her previous complaints that the Minister had apparently not disputed that secret investigations had been conducted in respect of her or that her sources had been identified through access to her call list. The Committee informed the applicant on 10 October 2016 that, on the basis of documents provided by the National Defence Service, there was no appearance of a breach of the law.

17. On 8 May 2017 the applicant submitted a request to the National Defence Service under Act no. CLV of 2009 on the Protection of Classified Data for leave to access documents in respect of the covert information gathering in the proceedings against T. Following a negative reply on the grounds that the disclosure of the requested information would jeopardise the prevention and/or investigation of crime, the applicant brought an action against the National Defence Service for judicial review. In a counterclaim,

the National Defence Service submitted that providing the requested information would allow the applicant to gain insight into the functioning of the Service and would divulge information about other persons likewise concerned by the covert information gathering. Furthermore, the requested information might be used in the criminal proceedings against T. The National Defence Service also put forward that, in any event, the covert information gathering had been lawful and had been authorised by a judge. The identity of the persons in respect of whom such measures were authorised constituted classified information.

18. In a final judgment of 11 September 2017 (in which T. was identified as the applicant's husband), the Budapest Administrative and Labour Court dismissed the action, holding that the applicant, quite independently of any conjecture on her part, had not been entitled to learn the identity of the person in respect of whom the covert information gathering had been ordered. This consideration precluded any further examination of her claims related to the lack of a judicial authorisation, the protection of her private life and of her freedom of expression and journalistic sources.

19. On 25 May 2018 the criminal court cleared T. of the charge of abuse of authority and the acquittal was upheld by the Budapest Court of Appeal on 12 December 2018.

RELEVANT LEGAL FRAMEWORK

I. DOMESTIC LAW

20. The relevant parts of the Data Protection Act of 2011 provide as follows:

Investigation by the [National Data Protection] Authority
Section 52

"(1) Every person shall have the right to notify the Authority and request an investigation in relation to an alleged infringement of his or her personal data or of the exercise of the rights of access to public information or information of public interest, or if there is imminent danger of such an infringement.

..."

Administrative proceedings for data protection
Section 60

"(1) In order to give effect to the right to protection of personal data, the Authority shall, upon a request by the data subject, open administrative proceedings for data protection and may open such proceedings for data protection of its own motion.

..."

21. The Civil Code of 2013 provides as follows, in so far as relevant:

Article 2:42
[Protection of rights relating to personality]

"(1) Everyone is entitled to freely exercise his or her personality rights ... and not to be impeded by others in exercising such rights.

(2) Human dignity and the related personality rights must be respected by all. Personality rights shall be protected under this [Code]. ..."

Article 6:548
[Liability for the actions of administrative authorities]

"(1) Liability for damage caused within the scope of administrative jurisdiction shall be established if the damage results from actions or omissions in the exercise of public authority and if the damage cannot be abated by way of common remedies or administrative actions.

(2) Liability for damage caused within the scope of administrative jurisdiction shall lie with the legal person exercising public authority. ..."

Article 6:549
[Liability for the actions of courts, public prosecutors, notaries public and court bailiffs]

"(1) The provisions on liability for damage caused within the scope of administrative jurisdiction shall apply, *mutatis mutandis*, to liability for the actions of courts and public prosecutors ..."

22. Act no. XIX of 1998 on the Code of Criminal Procedure provides, in so far as relevant:

Article 206/A

"...

(4) The admission of the results of covert information gathering as evidence in criminal proceedings, if the conditions set forth in paragraph (1) are met, may be requested by the prosecutor after the initiation of the investigation. The investigating judge shall decide on such a request."

23. The relevant parts of the Police Act (no. XXXIV of 1994) provide:

Chapter VII
Covert information gathering subject to judicial authorisation
Section 69

"(1) In the case of serious crimes and in the circumstances listed in subsection (3), the police may, subject to authorisation given by a judge and prior to the opening of a criminal investigation,

...

(d) obtain information on the content of communications transmitted *via* electronic telecommunication services and record such content; and

(e) obtain, record and use the information transmitted *via* an IT device or an IT system or stored thereon.

...”

Section 72

“(1) If the authorisation for using special measures would cause a delay that would clearly jeopardise the interest in successful prosecution, the chief of the police department may order a covert search and, for a maximum period of seventy-two hours, the use of special measures (an emergency order).

(2) In the event of an emergency order, an application for the authorisation shall be submitted at the same time. If the application is rejected, a new emergency order for the same purpose may not be issued on the basis of the same reasons or facts.”

Section 73

“...

(3) Any information unrelated to the subject matter and the personal data of any person who is not concerned with the case must be deleted within eight days from the termination of the covert information gathering using a special device.”

Section 92

“(1) A person whose fundamental right has been infringed through a violation of an obligation, a police measure, a failure to take a police measure or the use of coercive means as specified in Chapters IV-V, with the exception of sections 46/A-46/C, and in Chapter VI may:

(a) file a complaint with the police entity implementing the measure;

(b) request that his/her complaint is adjudicated by:

(ba) the national police chief;

(bb) the director general of the police entity for internal crime prevention and crime detection; or

(bc) the director general of the anti-terrorist entity.

...”

24. Under section 11(5) of the National Security Act, complaints about the activities of the National Security Services are to be investigated by the Minister of the Interior, who must inform the complainant of the outcome of the investigation and of the relevant measures within thirty days (this deadline may be extended once by another thirty days). Where a complainant does not accept the results of the investigation under section 11(5), the National Security Committee of Parliament may investigate a complaint of unlawful activities on the part of the National Security Services if, on the basis of an affirmative vote of at least one-third of the Committee members, the gravity of the complaint justifies an investigation. In investigating a complaint, the Committee must examine the complaint in issue and may request the Minister to submit his or her opinion on the case. If the Committee is of the view that

the operations of the National Security Services have been unlawful or improper, it may request the Minister to conduct investigations and to inform the Committee of the results of the investigations or may itself carry out factfinding investigations if it suspects that the operations of the services in question are contrary to the relevant laws. In carrying out the fact-finding investigations, the Committee may inspect the relevant documents in the records of the National Security Services and may hear evidence from staff members of the services in question. Depending on the findings, the Committee may invite the Minister to take the necessary actions.

II. DOMESTIC PRACTICE

25. The *Kúria*'s decision in case no. Bhar. 702/2019/9 contains the following relevant passage:

> "...The prohibition on the storage of information ... does not mean that the results of a lawfully authorised and implemented covert information-gathering measure which is not part of the criminal proceedings cannot be used once the presumed time-limit for lodging a criminal complaint has passed. It only means that information obtained, without judicial authorisation and without a legal basis, about other persons not concerned by the secret information gathering cannot be collected and stored. The *Kúria* merely points out that the courts trying criminal cases and the judges authorising covert information gathering have no way of verifying whether the services gathering the information have fulfilled their duty under section 73(3) of the Police Act to delete the information.
>
> ..."

26. Judgment no. Bf.133/2021/8 of the Budapest Court of Appeal contains the following relevant passages:

> "...
>
> It is the view of the second-instance court that the activities of covert information gathering and covert data acquisition – despite a number of similarities in their regulation – are considerably different in respect of the aims of the measures and the purpose of the relevant legal institutions. Covert information gathering for the purpose of suppressing criminal activity may only be ordered prior to the opening of the criminal proceedings and outside the criminal proceedings, under section 63(1) of the Police Act, for, among other purposes, the prevention, detection and disruption of criminal activity. The reason for this is that the essential condition for the opening of criminal proceedings, namely the suspicion that someone has committed a criminal offence – that is, the suspicion of particular conduct – is absent. At the time of the application of the covert measures, the information available to the authorities is restricted. In many cases the offence has not been committed yet, and therefore the identity of the persons involved is also unknown. One cannot speak of either offenders or suspects. It follows that while covert data acquisition may be authorised in respect of a suspect – a person who is suspected of committing a criminal offence – or a person who maintains a criminal relationship with a suspect, pursuant to section 202(1)-(2) of Act no. XIX of 1998, covert information gathering is not limited to these persons. Accordingly, ... for the authorisation of covert information gathering, it is not necessary that the identity of the person concerned be known to the authorities. It follows that covert information

gathering may be regulated through the setting of time-limits, which is the only element which the authorities may be held accountable for. The balance between the interest in the prosecution of criminal offences and fundamental rights is ensured by defining in law the offences in respect of which covert information gathering may be ordered, by prescribing time-limits, by requiring judicial authorisation both for ordering and prolonging a measure, by providing for an obligation to discontinue the measure, by setting conditions for the use of its results and by penalising a failure to lodge a criminal complaint ..."

THE LAW

I. ALLEGED VIOLATION OF ARTICLES 8 AND 10 OF THE CONVENTION

27. The applicant complained under Articles 8, 10 and 13 of the Convention about the tapping of her telephone calls and that she had been denied an effective remedy in that connection. The Court being the master of the characterisation to be given in law to the facts complained of (see *Radomilja and Others v. Croatia* [GC], nos. 37685/10 and 22768/12, § 126, 20 March 2018) considers that by its very nature, the applicant's argument presented under Article 13 of the Convention falls to be examined under the merits of her complaint under Articles 8 and 10 of the Convention, in particular in terms of whether sufficient safeguards were put in place to ensure the applicant's rights under those provisions. Although questions raised by surveillance measures are usually considered under Article 8 alone, in the present case they are so intertwined with the issue raised under Article 10 that the Court finds it appropriate to consider the matter under Articles 8 and 10 concurrently (see *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, § 88, 22 November 2012). The Articles in question read as follows:

Article 8

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Article 10

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

A. Admissibility

1. The parties' submissions

28. The Government argued that the applicant could not claim to be a "victim" for the purposes of Article 34 of the Convention since it had not been her telephone, but rather that of T., which had been tapped. Moreover, it had been T. and not the applicant who had been subjected to criminal prosecution. Neither the applicant nor her employer had been penalised for publishing the information obtained from her contact in the police.

29. Moreover, she had not exhausted domestic remedies in that she had not pursued a complaint procedure with the National Authority for Data Protection and Freedom of Information ("the Data Protection Authority" or "the DPA") under sections 52 or 60 of the Data Protection Act of 2011.

30. The Government further argued that the applicant could have sued the responsible authorities for damages on account of the infringement of her right to freedom of expression under the relevant rules of the Civil Code – a procedure capable of leading to a judgment which could ultimately have been challenged before the Constitutional Court.

31. The applicant alleged that the fact that the domestic authorities had opened criminal investigations in respect of T. proved that T. had been identified as her source in the police. In her understanding this demonstrated a reasonable likelihood that her communications had been intercepted and her call lists had been monitored.

32. The applicant further submitted that she had actively sought remedies for the alleged tapping of her phone. She initiated criminal proceedings, but her criminal complaint had been dismissed by the Police Department. She had enquired with the Ministry of Interior and the National Security Committee of Parliament; none of them had conducted an adequate examination of the matter. She had lodged a complaint with the National Defence Service and subsequently requested access to the documents in respect of the covert information gathering in the proceedings against T. These actions had also been to no avail, thus she eventually challenged the alleged grievances before the courts.

33. She argued that the legal avenues referred to by the Government, that is, having recourse to the DPA and to a civil action, would have been no more effective than the ones she had already availed herself of.

2. The Court's assessment

34. The Court reiterates that, in the event of there being a number of domestic remedies which an individual can pursue, that person is entitled to choose a remedy which addresses his or her essential grievance. In other words, when a remedy has been pursued, use of another remedy which has essentially the same objective is not required (see *Moreira Barbosa v. Portugal* (dec.), no. 65681/01, ECHR 2004-V (extracts), and *Leja v. Latvia*, no. 71072/01, § 46, 14 June 2011). In the present case, the Court is satisfied that the applicant repeatedly brought her grievance to the attention of the national authorities, albeit in vain. In particular, she complained to the Pest County Police Department, the National Defence Service, the Minister of the Interior, the National Security Committee of Parliament and, lastly, to the administrative court. The Government did not question the effectiveness of these legal avenues in the applicant's circumstances.

35. In any event, as to the Government's argument that the applicant should have brought her complaint before the DPA, the Court notes that in *Hüttl v. Hungary* ([Committee], no. 58032/16, 29 September 2022, cited for illustrative purposes), in the context of Article 8 of the Convention, it addressed the availability and adequacy of a DPA investigation and the question whether such an investigation represented safeguards capable of bringing a surveillance measure into line with the requirements of Article 8 of the Convention. The essence of the finding of a violation of Article 8 was that – because of the limited power conferred on the DPA and the resultant absence of external, independent scrutiny in such matters – the Court was not convinced that the safeguard suggested by the Government was capable of rendering the relevant Hungarian legislation sufficiently precise, effective and comprehensive as to the ordering, execution and potential redressing of surveillance measures (ibid., § 18).

36. The remainder of the Government's arguments revolved around the availability of a civil action. The Court notes at the outset that the Government did not provide any examples of domestic case-law demonstrating that a civil action has proved effective in similar cases and would therefore constitute a remedy both effective and available in practice (see, *mutatis mutandis*, *Ádám and Others v. Romania*, nos. 81114/17 and 5 others, § 49, 13 October 2020). Moreover, the Court cannot find, in the material submitted before it, any indication of the prospects of success of this remedy. It cannot assess in the abstract how the domestic courts would have dealt with an action brought by the applicant in respect of the infringement of her right to freedom of expression due to secret surveillance measures. The Court finds no justification for the complete absence of domestic case-law from the Government's submissions.

37. Consequently, the application cannot be rejected for non-exhaustion of domestic remedies.

38. Concerning the applicant's victim status, the Court notes that while the Government contested that the applicant's rights had been interfered with on the grounds that it was not her but T. who had been the target of the phone tapping, these arguments related to the phone tapping of T. in the course of the criminal proceedings conducted against him (see paragraph 7 above). However, the Government did not offer any explanation as to the alleged monitoring of the applicant's conversations prior to the granting of authorisation to apply secret surveillance measures in respect of T. (see paragraph 66 below). At the very least, they did not rebut the applicant's contention that covert information gathering had been ordered in respect of her prior to the tapping of T.'s phone. Considering in addition the nature of the applicant's complaint (see paragraph 56 below), the Court is of the view that the applicant can claim to be victim of a violation of her rights under the Convention within the meaning of Article 34 of the Convention.

39. The Court further considers that the application is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicant

40. The applicant submitted that her mobile phone had been tapped and her conversations intercepted in order for the authorities to identify her police sources. Apart from the obvious repercussions on her private life as protected by Article 8 of the Convention, the measure had, importantly, undermined the protection of journalistic sources protected by Article 10 of the Convention. She further argued that the phone tapping had in fact been directed against her rather than against T. and had from the outset been aimed at identifying her sources.

41. The applicant maintained that there were reasonable grounds to believe that she had been subjected to unlawful interception. She put forward several factors in support of her argument. Firstly, she had been a journalist for a number of years and in 2015 she had published several press reports on various high-profile murder cases, disclosing information that went beyond what other media content providers had known about. This had necessarily triggered the attention of the police. Secondly, the judicial authorisation of the tapping of T.'s phone had been issued in respect of criminal activity that necessarily presupposed an additional, civilian perpetrator other than T. Thirdly, the numbering of the documents in T.'s case file indicated that other decisions authorising surveillance measures had already been given in the case. Fourthly, the Government had not denied that secret surveillance measures had been authorised in respect of the applicant. Fifthly, T. had been

charged with disclosure of information concerning a murder case on the basis of evidence acquired through the tapping of T.'s phone; this had only been possible because T. had already been identified as her source through the previous tapping of her own phone. Sixthly, T. had been acquitted for unknown reasons. In the applicant's understanding, the grounds for acquitting T. had been that the only evidence against him – the results of the covert phone tapping – had been acquired unlawfully.

42. The applicant also argued that knowledge of the circumstances of the covert information gathering had lain exclusively with the domestic authorities, and thus the burden of proof rested with the Government to provide a satisfactory and convincing application. The Government had not provided any plausible explanation as to how T. had been identified as a suspect, that is, a member of the police who had been leaking information.

43. The applicant accepted that there was a legal basis in domestic law for covert information gathering. However, she argued that the domestic judicial authorities should have assessed the competing interests of protecting journalistic sources and detecting crime. However, the investigating authorities had circumvented the preliminary judicial assessment by using unauthorised means of surveillance. The applicant further disputed the legitimate aim pursued by the measures complained of, as, in her view, they had been applied in order to disclose her source of information rather than to prevent any crime.

44. In the applicant's view, the need to unmask a disloyal officer of a law-enforcement authority had not constituted an overriding public interest and had not outweighed the need to protect journalistic sources.

45. In addition, she submitted that there had been no procedure attended by adequate legal safeguards to enable an independent assessment as to whether the interest of the criminal investigation had overridden the public interest in the protection of journalistic sources.

(b) The Government

46. In the Government's parlance, the secret surveillance of T. had had a legal basis in domestic law and had been authorised by a judge. It had been limited to the bare minimum necessary to build a case against him. Thus, the measure had been applied in a proportionate manner.

47. Even if the measure could be seen in the light of interference with freedom of expression, that freedom did not entail the right of a police officer to breach his official duties. It was not limitless and could not undo the boundaries set by the confidentiality of police work. Likewise, the protection of journalistic sources was not absolute and was restricted to situations where the information was received lawfully. Thus, that protection was not applicable where a journalist had attempted to obtain information by committing a criminal act, such as by bribing a police officer.

48. The Government asserted, moreover, that the applicant had not been seeking to impart information on a matter of public debate but had rather been gathering elements for a sensationalistic article in the tabloid press. Therefore, the interest of the State in detecting criminal acts had been more important than the applicant's interest in transmitting the information in question to the public.

2. The Court's assessment

(a) General principles

49. The Court reiterates that (i) telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8, (ii) their monitoring amounts to an interference with the exercise of the rights under Article 8, and (iii) such interference is justified by the terms of paragraph 2 of Article 8 only if it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is "necessary in a democratic society" in order to achieve the aim or aims (see *Potoczká and Adamčo v. Slovakia*, no. 7286/16, § 69, 12 January 2023).

50. In the context of Article 8, the Court has found that in cases where the legislation permitting secret surveillance is contested before it, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of the law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 236, ECHR 2015, and *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, § 334, 25 May 2021).

51. In this connection it should be reiterated that in its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: (i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed (see *Roman Zakharov*, cited above, § 231).

52. As regards Article 10, the Court reiterates that the protection of journalistic sources is one of the cornerstones of freedom of the press.

Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result, the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be adversely affected (see, among other authorities, *Goodwin v. the United Kingdom*, 27 March 1996, § 39, *Reports of Judgments and Decisions* 1996-II, and *Sanoma Uitgevers B.V. v. the Netherlands* [GC], no. 38224/03, § 50, 14 September 2010).

53. Any interference with the right to protection of journalistic sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake. First and foremost among these safeguards is the guarantee of a review by a judge or other independent and impartial decision-making body with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not (see *Sanoma Uitgevers B.V.*, cited above, §§ 88-90).

54. Given the preventive nature of such review, the judge or other independent and impartial body must be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be assessed properly. The decision to be taken should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of journalist's sources. In situations of urgency, a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk (see *Big Brother Watch and Others*, cited above, §§ 444-45, and *Sanoma Uitgevers B.V.*, cited above, § 92).

(b) Application of those principles to the present case

55. In the present case the applicant complained specifically about her being targeted by the secret surveillance measure prior to the tapping of T.'s phone and adduced a number of arguments in support of her complaint (see paragraph 41 above).

56. The Court also observes that the applicant's contention was that although she had brought to the attention of the national authorities the essence of her grievances, her claims had not been entertained at any level of jurisdiction. She also suggested that her status as a journalist had required that

the domestic authorities carry out a balancing of her right to the protection of her journalistic sources and the interests attached by the authorities to the successful prosecution of the perpetrator. In her view there had been no procedure attended by adequate legal safeguards to enable such balancing (see paragraph 45 above). Moreover, the interception of her communication had been unlawful since it had not been authorised by a judge.

57. Given the nature of the applicant's complaint, the Court will turn to the question whether the domestic proceedings were attended with legal procedural safeguards providing the applicant with the requisite protection of her interests.

58. As regards the applicant's allegation that her phone had been tapped without a relevant judicial decision (see paragraph 43 above), bearing in mind the findings in paragraph 67 below, the Court cannot rule on the question whether the investigating authorities implemented secret surveillance measures in respect of the applicant or, if so, whether they circumvented the requirement of judicial authorisation foreseen under domestic law (see paragraph 23 above).

59. However, the question whether the applicant was able to complain in an effective manner about the alleged ordering of the surveillance measure and the alleged absence of judicial authorisation is a separate issue to which the Court will revert below.

60. The Court reiterates in this connection its previous finding that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies (see *Weber and Saravia v. Germany,* (dec.), no. 54934/00, §135, 29 June 2006, and *Roman Zakharov*, cited above, § 286). The Court finds it relevant that in Hungarian law no provision was made for any form of notification of secret surveillance measures, not even in cases in which notification could be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure (see *Roman Zakharov*, cited above, § 287). The Court therefore accepts that the applicant was unlikely to find out whether her communications had been intercepted, making it inherently difficult for her to eventually seek a remedy for the presumed measure.

61. It does not appear either that the applicant had access to an independent and impartial body with jurisdiction to examine any complaint of unlawful interception, independently of a notification that such interception had taken place (compare Kennedy v. the United Kingdom, no. 26839/05, § 167, 18 May 2010), as demonstrated by the facts of the present case.

62. Namely, the applicant raised her concerns about the monitoring of her telephone conversations with the National Defence Service under the Police Act (see paragraph 13 above), the Minister of the Interior and the National Security Committee of Parliament under the National Security Act (see paragraphs 15 and 16 above), arguing that the secret surveillance measure

had been used in respect of her and had been applied without judicial authorisation. Lastly, she requested leave to access the documents produced in the context of the criminal proceedings against T. from the National Defence Service and, subsequently, from the Budapest Administrative and Labour Court, seeking access to information about the surveillance measures (see paragraphs 17 and 18 above).

63. However, none of these authorities provided any clarification as to the question whether the applicant had been subjected to covert information gathering and if so, whether the measure had been proportionate to her individual circumstances and whether it had been authorised by a judge.

64. Firstly, the applicant's complaint could not be entertained under the Police Act, since no remedy lay against measures related to covert information gathering (see paragraphs 14 and 23 above).

65. As to the Minister of the Interior and the National Security Committee, it is certainly true that the applicant was permitted to apply to those authorities on the basis of her suspicion that her communications had been intercepted, even in the absence of a notification of interception (see, in this respect, *Roman Zakharov*, cited above, § 234).

66. The Court already raised concerns in *Szabó and Vissy v. Hungary* (no. 37138/14, §§ 83, 86 and 88, 12 January 2016) about these oversight mechanisms for the lack of the Minister's independence, the lack of subsequent notification of any kind and for the lack of any practical example demonstrating the effectiveness of these avenues. The Court further doubts whether they constituted adequate safeguards in the applicant's presumed situation, where the information on the authorisation of covert information gathering remained confidential and therefore inaccessible to the person concerned.

67. Indeed, both of those authorities gave only general assurances to the applicant about the lawful functioning of the National Security Service, without addressing her grievances, including the question whether such measures had taken place and whether they had been carried out lawfully and in respect of the applicant's interests as a journalist.

68. Moreover, it does not appear that such general statements on the lawful functioning of the National Security Services were to reflect any balancing between the seriousness of the criminal offence being prosecuted, on the one hand, and the potentially chilling effect that a secret information-gathering order might have on the exercise of the freedom of the press, on the other.

69. Finally, it appears, as noted in paragraph 23 above, that prior to the commencement of the criminal investigation, covert information gathering could be ordered under section 69 of the Police Act. The Police Act, as explained by the Budapest Court of Appeal (see paragraph 26 above), allowed for the measure without any restrictions as to the persons subject to those measures. Indeed, while the legislation set out the criminal offences which

could give rise to interception, it did not describe the categories of persons who could be subjected to surveillance and did not provide for exceptions or limitations.

70. The Court is not reassured that that provision allowed any consideration to be given to whether the interception of communications involved confidential journalistic sources, or that it was open to the judge to refuse to authorise a measure so as to protect sources from being revealed (see *Sanoma Uitgevers B.V.*, cited above, § 92). Neither did the provision require any balancing of the aims pursued by the application of secret surveillance measures and the ramifications of the tapping of a journalist's telephone.

71. In light of the considerations above, and in particular the domestic authorities' failure to address the applicant's grievances, the Court thus does not find that adequate procedural safeguards were in place for the applicant to challenge the alleged use of secret surveillance against her with a view to discovering her journalistic sources.

There has therefore been a violation of Articles 8 and 10 of the Convention.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

72. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

73. The applicant claimed 25,000 euros (EUR) in respect of non-pecuniary damage.

74. The Government contested that claim.

75. The Court awards the applicant, on an equitable basis, EUR 6,500 in respect of non-pecuniary damage, plus any tax that may be chargeable.

B. Costs and expenses

76. The applicant also claimed EUR 11,205 plus VAT for the costs and expenses incurred before the Court, corresponding to 71.9 hours of legal work and 8.4 hours of paralegal work.

77. The Government contested that claim.

78. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its

possession and the above criteria, the Court considers it reasonable to award the sum of EUR 7,000 covering costs under all heads, plus any tax that may be chargeable to the applicant.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Articles 8 and 10 of the Convention;

3. *Holds*
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
      (i) EUR 6,500 (six thousand five hundred euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
      (ii) EUR 7,000 (seven thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 28 November 2024, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Ilse Freiwirth Registrar	Marko Bošnjak President