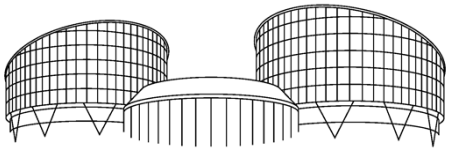

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF SEDLETSKA v. UKRAINE

(Application no. 42634/18)

JUDGMENT

Art 10 • Freedom of expression • Protection of journalistic sources • Interference with applicant's rights due to judicially authorised access to her mobile telephone communications data not "necessary in a democratic society": grossly disproportionate and not justified by an "overriding requirement in the public interest"

STRASBOURG

1 April 2021

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 Sedletska v. Ukraine,

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

Síofra O'Leary, *President,*
Stéphanie Mourou-Vikström,
Lətif Hüseynov,
Lado Chanturia,
Ivana Jelić,
Arnfinn Bårdsen, *judges,*
Sergiy Goncharenko, ad hoc *judge,*
and Victor Soloveytchik, *Section Registrar,*

Having regard to: the application (no. 42634/18) against Ukraine lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Ukrainian national, Ms Nataliya Yuriyivna Sedletska ("the applicant"), on 10 September 2018;

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

the decision to indicate an interim measure to the respondent Government under Rule 39 of the Rules of Court;

the withdrawal of Ganna Yudkivska, the judge elected in respect of Ukraine, from sitting in the case (Rule 28 § 3 of the Rules of Court) and the decision of the President of the Section to appoint Mr Sergiy Goncharenko to sit as an ad hoc judge (Article 26 § 4 of the Convention and Rule 29 § 1 (a));

the observations submitted by the respondent Government and the observations in reply submitted by the applicant;

the comments submitted by the Media Legal Defence Initiative and Human Rights Platform, who were granted leave to intervene by the President of the Section under Article 36 § 2 of the Convention and Rule 44 § 3 of the Rules of Court;

Having deliberated in private on 9 March 2021,

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

INTRODUCTION

1. The present case concerns complaints raised under Articles 10 and 13 of the Convention of interference with the protection of journalistic sources as a result of judicial authorisation being given to the investigative authorities to access the applicant's communications data stored by her mobile telephone operator and lack of effective remedies in respect of her relevant complaint.

THE FACTS

2. The applicant was born in 1987 and lives in Kyiv. She was represented by Mr S. Zayets and Ms L. Pankratova, lawyers practising in Irpin and Kyiv respectively.

3. The Government were represented by their Agent, Mr I. Lishchyna.

4. The facts of the case, as submitted by the parties, may be summarised as follows.

I. THE CIRCUMSTANCES OF THE CASE

A. Background of the case

5. The applicant is a journalist at the Kyiv office of Radio Free Europe/Radio Liberty. She is also the editor-in-chief of the "Schemes: Corruption in Detail" television programme. The programme has been running since 2014 and many of its issues concern senior prosecutors and politicians.

6. In 2015 the National Anticorruption Bureau of Ukraine ("the NABU") instituted criminal proceedings against a prosecutor, K., on suspicion of unjust enrichment. In the framework of those proceedings, in the period between May and July 2016, the NABU tapped the telephone of Ms N., K.'s partner.

7. In 2017 K. started working at the Prosecutor General's Office ("the PGO").

8. On 13 November 2017 the *Obozrevatel* media website published an article stating that in the summer of 2017 the head of the NABU, S., had held a closed meeting with some media representatives during which he had disclosed confidential information about some ongoing criminal investigations, including the one against K. It was apparent from this article that, among other things, the media representatives had listened to a recording of a taped telephone conversation between Ms N. and her acquaintance, in which the two of them were discussing details of Ms N.'s private life. The *Obozrevatel* article was accompanied by an audio file presented as the audio recording of that meeting, including the recording of Ms N.'s telephone conversation with her acquaintance.

9. The same day M., a Member of Parliament, complained to the Prosecutor General that the above article was unlawful and had indicated that S. had also breached the rules of confidentiality pertaining to ongoing criminal proceedings, as well as Ms N.'s right to respect for her private life in divulging information about her to the journalists.

10. On 15 November 2017 Ms N. also complained to the PGO about the same matter, asking that criminal proceedings be instituted against S. and

his colleagues for breaching her privacy and making public the material of the ongoing criminal investigations.

B. Criminal investigation of alleged misconduct by S.

11. On 16 November 2017 the PGO instituted criminal proceedings against S. under Articles 163, 182, 328 and 387 of the Criminal Code for violation of privacy and disclosure of confidential information concerning ongoing criminal investigations.

12. On 22 November 2017 the PGO requested that the Security Service of Ukraine ("the SSU") conduct a voice recognition analysis of those present at the purported meeting with S. using the audio recording featured in the article on the *Obozrevatel* media website.

13. On 4 December 2017 the SSU informed the PGO of the results of the voice recognition analysis. It was mentioned that the voices on the recording were likely to belong to S., his deputy U. and two journalists, B. and the applicant. There were also several other voices which could not be identified.

14. On 19 December 2017 the applicant was summoned to the PGO for questioning. She informed the investigator, I. ("the investigator") that, as a journalist, she communicated with many law-enforcement officials, including S. Information received from public events was used in her professional work. As to the information received confidentially, she claimed that, under Article 65 of the Code of Criminal Procedure, she could not be interviewed as a witness if it would lead to the identification of her journalistic sources. For the same reason, she refused to answer questions related to the alleged meeting with S. and to either confirm or deny her own presence at that meeting.

C. PGO's request for access to the applicant's communications data and ensuing events

15. On 27 August 2018 a PGO investigator submitted a request to the Pecherskyy District Court in Kyiv ("the District Court") for access to the applicant's communications data from 19 July 2016 (the date when the results of Ms N.'s phone tapping were formally documented) to 16 November 2017 (the date of institution of the criminal proceedings against S.) held by the mobile service provider JSC "Kyivstar". The requested data included dates, times, call durations, telephone numbers, sent and received text messages (SMS, MMS), and the location of the applicant at the time of each call or message. The information was requested in order to establish the exact time and place of the meeting with S.

16. The same day P., an investigating judge of the District Court ("the investigating judge") examined the investigator's request and issued an

order authorising the collection of the data requested. It was noted in the order, in particular, that under Article 163 of the Code of Criminal Procedure (CCP) it was possible to examine the matter without the applicant being summoned, as there were "sufficient reasons to believe that there existed a real threat of the information sought being altered or destroyed". The order stated that it was not subject to appeal and was valid for one month.

17. On 1 September 2018 an article on the *Court Reporter* media website stated that the PGO had started checking telephone calls made by [unnamed] journalists who had supposedly been present at the purported meeting with S. The site referred to the order of the investigating judge of 27 August 2018, and contained a link to an anonymised version of that order in the Unified State Register of Court Decisions. The article was accompanied by individual pictures of S. and a number of journalists and human rights activists, including the applicant.

18. On 4 September 2018 the PGO investigator wrote a letter to the mobile service provider JSC "Kyivstar" referring to the District Court's order of 27 August 2018 and informing the addressee that data was only required about the dates, times and location of the mobile telephones of the applicant and one other person - apparently, B., - near the six specified streets and places in Kyiv. It was also indicated that this information should be provided without any other data being disclosed.

19. On 7 September 2018 the applicant and her lawyer asked the District Court for a copy of the order of 27 August 2018. The request was refused on 10 September 2018.

20. On 11 September 2018 the applicant, notwithstanding the fact that the order of 27 August 2018 indicated that it was not possible to lodge an appeal against it, challenged it before the Kyiv City Court of Appeal ("the Court of Appeal") and requested its suspension.

21. On 15 September 2018 the Prosecutor General was asked during a press conference about the data sought from the mobile telephones of the applicant and B. He stated that while the freedom of journalistic activity was of paramount importance, some interference with it was justified owing to the lack of alternative means of obtaining information about the date on which the meeting of S. with journalists had taken place. He stated that information was only required from one cell of the mobile network, namely that covering the NABU offices. Nevertheless, he argued that the period of sixteen months was justified. He also stated that he was in principle ready to show the reply from the mobile service provider to make it apparent that no data identifying any journalistic sources had been either claimed or received.

22. On 18 September 2018 the Court of Appeal found it possible to accept the applicant's appeal against the order of 27 August 2018 for consideration. It noted that court orders authorising "access to items and

documents" under Article 163 of the CCP were, as a general rule, not amenable to appeal. However, Article 309 of the CCP envisaged an exception for cases, where such an order would entail seizure of items or documents, without which an individual entrepreneur or a legal entity would be unable to carry out their activity. Referring, in particular, to the importance of the journalistic sources for the applicant's professional activity, the Court of Appeal decided that this exception could be applied in her case. The court further noted, referring, in particular, to Article 8 of the Convention and Section 17 of the *State Support of Mass Media and Social Protection of Journalists Act*, that the investigating judge of the District Court had not given proper reasons for the disputed order and had not complied with the requirements of domestic law, in violation of the applicant's rights. The Court of Appeal considered, however, that the scope of the data requested in the investigator's letter of 4 September 2018 was not excessive. It quashed the District Court's order and made a new one authorising access to data about the dates and time of presence of the applicant's mobile telephone on six specified streets and places in Kyiv during the period from 19 July 2016 to 16 November 2017. The relevant part of the order read as follows:

> "... as correctly noted by the appellant, and as the judicial panel agrees, the investigative judge issued the order for temporary access ... without due reason, failing to comply with legislative requirements, in breach of the [applicant's] rights, as a journalist, protected by law.
>
> At the same time, as the prosecutor explained at the hearing, such measures were used with a view to achieving efficiency in the aforementioned criminal proceedings, in particular, in order to establish more exactly the time and place of the commission of an offence, ... since, being questioned as a witness, [the applicant] had refused to give a statement to the investigation in this regard.
>
> In addition, it can be seen from the letter of [the PGO investigator] of 4 September 2018 ... that the latter was only asking for permission to access data concerning dates and times and the location of the [applicant's telephone] between 19 July 2016 and 16 November 2017 within the boundaries of the base stations of the operator located in Kyiv on the [following] streets: Surikova [Street], Bogdanivska [Street], Shovkunenka [Street], ... Lypkivskogo [Street], Khomova Lane, Povitroflotskiy Avenue, Solomyanska Square and the [area covered by these stations].
>
> The judicial panel considers that allowing the aforementioned request by the investigator in this particular aspect shall correspond to the task of the criminal investigation to ensure a prompt, comprehensive and unbiased inquiry and will sufficiently safeguard the protected rights and lawful interests of the [applicant] as a journalist."

23. On 20 September 2018 the applicant and her lawyer asked the mobile service provider JSC "Kyivstar" and the PGO whether the investigation had had access to the applicant's mobile telephone data in accordance with the orders of 27 August and 18 September 2018. Fifteen NGOs and the media made a "flash mob" requesting the same information

from the PGO. All these requests were refused on the basis of the confidentiality of the ongoing investigation.

II. PROCEDURE BEFORE THE COURT

24. On 10 September 2018 the applicant asked the Court for the indication of an interim measure under Rule 39 of the Rules of the Court.

25. On 18 September 2018 the Court indicated to the Government under Rule 39 of the Rules of the Court that, in the interests of the parties and the proper conduct of the proceedings, they should ensure that the public authorities abstain from accessing any of the data specified in the order of 27 August 2018 concerning the applicant.

26. On 27 September 2018, when interviewed during a visit to Parliament, the Prosecutor General stated that no data had been received from the mobile telephone operator, that they had complied with the decision of the Court [regarding the indicated interim measure] but that they would need the data to investigate a serious crime and would try to explain this to the Court.

27. On 16 October 2018 the Court extended the aforementioned interim measure indicating to the Government of Ukraine to ensure that the public authorities abstain from accessing any data mentioned in the ruling of 18 September 2018 by the Kyiv City Court of Appeal concerning the applicant until further notice.

28. On 12 February 2019 the PGO informed the Government's Agent within the framework of the present proceedings that they had not carried out any of the actions authorised by the orders of 27 August and 18 September 2018 in the applicant's case, taking into account the requirements imposed under Rule 39.

RELEVANT LEGAL FRAMEWORK

I. RELEVANT DOMESTIC LAW

A. Constitution of Ukraine

29. Article 34 of the Constitution of Ukraine reads:

> "Everyone is guaranteed the right to freedom of thought and speech, and to the free expression of his or her views and beliefs.
>
> Everyone has the right to freely collect, store, use and disseminate information by oral, written or other means of his or her choice.
>
> The exercise of these rights may be restricted by law in the interests of national security, territorial indivisibility or public order, with the purpose of preventing disturbances or crimes, protecting the health of the population, the reputation or rights of other persons, preventing the publication of information received confidentially, or supporting the authority and impartiality of justice."

B. Criminal Code

30. The relevant provisions of the Code concern the following offences:

- Article 163: Violation of privacy of mail, telephone conversations, telegraphs and other correspondence conveyed by means of communication or via computers;
- Article 182: Violation of personal privacy;
- Article 328: Disclosure of State secrets;
- Article 387: Disclosure of information on pre-trial investigation or inquiry.

C. Code of Criminal Procedure ("the CCP")

31. The relevant provisions of the Code provide as follows:

Article 65 – Witness

"...

2. The following persons may not be interviewed as witnesses:

...

(6) journalists, about confidential information of a professional nature provided on condition of non-disclosure of its author or source ..."

Article 163 – Consideration of a request for provisional access to items and documents

"1. Upon receiving a request for provisional access to items and documents, the investigating judge or court shall summon the person in possession of the items and documents, except in the case specified in [paragraph 2] of this Article.

2. If the party to criminal proceedings that filed the request proves that there are sufficient grounds to believe that a real threat exists of the items and documents concerned being altered or destroyed, the request may be considered by the investigating judge or court without the person in possession of them being summoned ... "

Article 309 – Rulings by an investigative judge, which can be appealed at the pre-trial investigation stage

"1. The following rulings by an investigative judge may be appealed at the pre-trial investigation stage:

...

10) [concerning] provisional access to items and documents, which authorise seizure of items and documents, ... in absence of which an individual entrepreneur or a legal entity will be deprived of an opportunity to carry out their activity; ...

...

3. Other rulings by an investigative judge may not be appealed against and objections against them may be submitted during preparatory hearing in court."

D. State Support of Mass Media and Social Protection of Journalists Act of 23 September 1997

32. The relevant part of section 17 of the Act provides as follows:

Section 17 – Liability for trespass or other actions against the life and health of a journalist and a journalist's liability for non-pecuniary damage caused by him/her

"... The professional activities of a journalist shall not serve as grounds for his or her arrest and detention, or for the seizure of material collected, processed and prepared by him or her or technical [equipment] that he or she uses in his or her work...".

II. RELEVANT INTERNATIONAL MATERIAL

33. Several international documents concern the protection of journalistic sources, including the *Resolution on Journalistic Freedoms and Human Rights*, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and the *European Parliament's Resolution on Confidentiality for Journalists' Sources* (18 January 1994, Official Journal of the European Communities No. C 44/34).

34. Recommendation No. R (2000) 7 on the right of journalists not to disclose their sources of information was adopted by the Committee of Ministers of the Council of Europe on 8 March 2000. The appendix contains principles concerning the right of journalists not to disclose their sources of information, including the following:

Definitions

"For the purposes of this Recommendation:

a. the term 'journalist' means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication;

b. the term 'information' means any statement of fact, opinion or idea in the form of text, sound and/or picture;

c. the term 'source' means any person who provides information to a journalist;

d. the term 'information identifying a source' means, as far as this is likely to lead to the identification of a source:

i. the name and personal data as well as voice and image of a source,

ii. the factual circumstances of acquiring information from a source by a journalist,

iii. the unpublished content of the information provided by a source to a journalist, and

iv. personal data of journalists and their employers related to their professional work.

Principle 1 (Right of non-disclosure of journalists)

Domestic law and practice in member States should provide for explicit and clear protection of the right of journalists not to disclose information identifying a source in accordance with Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: the Convention) and the principles established herein, which are to be considered as minimum standards for the respect of this right.

...

Principle 3 (Limits to the right of non-disclosure)

a. The right of journalists not to disclose information identifying a source must not be subject to other restrictions than those mentioned in Article 10 § 2 of the Convention. In determining whether a legitimate interest in a disclosure falling within the scope of Article 10 § 2 of the Convention outweighs the public interest in not disclosing information identifying a source, competent authorities of member States shall pay particular regard to the importance of the right of non-disclosure and the pre-eminence given to it in the case-law of the European Court of Human Rights, and may only order a disclosure if, subject to paragraph b, there exists an overriding requirement in the public interest and if circumstances are of a sufficiently vital and serious nature.

b. The disclosure of information identifying a source should not be deemed necessary unless it can be convincingly established that:

i. reasonable alternative measures to the disclosure do not exist or have been exhausted by the persons or public authorities that seek the disclosure, and

ii. the legitimate interest in the disclosure clearly outweighs the public interest in the non-disclosure, bearing in mind that:

• an overriding requirement of the need for disclosure is proved,

• the circumstances are of a sufficiently vital and serious nature,

• the necessity of the disclosure is identified as responding to a pressing social need, and

• member States enjoy a certain margin of appreciation in assessing this need, but this margin goes hand in hand with the supervision by the European Court of Human Rights.

c. The above requirements should be applied at all stages of any proceedings where the right of non-disclosure might be invoked.

Principle 4 (Alternative evidence to journalists' sources)

In legal proceedings against a journalist on grounds of an alleged infringement of the honour or reputation of a person, authorities should consider, for the purpose of establishing the truth or otherwise of the allegation, all evidence which is available to them under national procedural law and may not require for that purpose the disclosure of information identifying a source by the journalist.

...

Principle 6 (Interception of communication, surveillance and judicial search and seizure)

a. The following measures should not be applied if their purpose is to circumvent the right of journalists, under the terms of these principles, not to disclose information identifying a source:

i. interception orders or actions concerning communication or correspondence of journalists or their employers,

ii. surveillance orders or actions concerning journalists, their contacts or their employers, or

iii. search or seizure orders or actions concerning the private or business premises, belongings or correspondence of journalists or their employers or personal data related to their professional work.

b. Where information identifying a source has been properly obtained by police or judicial authorities by any of the above actions, although this might not have been the purpose of these actions, measures should be taken to prevent the subsequent use of this information as evidence before courts, unless the disclosure would be justified under Principle 3."

35. On 25 January 2011 the Parliamentary Assembly of the Council of Europe adopted Recommendation 1950 (2011), *The protection of journalists' sources,* which, *inter alia*, indicated as follows:

"5. Public authorities must not demand the disclosure of information identifying a source unless the requirements of Article 10, paragraph 2, of the Convention are met and unless it can be convincingly established that reasonable alternative measures to disclosure do not exist or have been exhausted, the legitimate interest in the disclosure clearly outweighs the public interest in the non-disclosure, and an overriding requirement of the need for disclosure is proved.

6. The disclosure of information identifying a source should therefore be limited to exceptional circumstances where vital public or individual interests are at stake and can be convincingly established. The competent authorities, requesting exceptionally the disclosure of a source, must specify the reasons why such vital interest outweighs the interest in the non-disclosure and whether alternative measures have been exhausted, such as other evidence. If sources are protected against any disclosure under national law, their disclosure must not be requested.

...

8. The right of journalists not to disclose their sources applies also to sources from within the police or judicial authorities. Where such provision of information to journalists was illegal, police and judicial authorities must pursue internal investigations instead of asking journalists to disclose their sources.

...

12. The Assembly reaffirms that the confidentiality of journalists' sources must not be compromised by the increasing technological possibilities for public authorities to control the use by journalists of mobile communication and Internet media. The interception of correspondence, surveillance of journalists or search and seizure of information must not circumvent the protection of journalists' sources. Internet service providers and communication companies should not be obliged to disclose

information which may lead to the identification of journalists' sources in violation of Article 10 of the Convention."

36. On 8 September 2015 the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression submitted a report to the UN General Assembly (A/70/361), which stated, *inter alia* (footnotes omitted):

"C. Nature and scope of protection

21. Some authorities refer to a journalistic 'privilege' not to disclose a source's identity, but both reporter and source enjoy rights that may be limited only according to article 19 (3). Revealing or coercing the revelation of the identity of a source creates disincentives for disclosure, dries up further sources to report a story accurately and damages an important tool of accountability. In the light of the importance attached to source confidentiality, any restrictions must be genuinely exceptional and subject to the highest standards, implemented by judicial authorities only. Such situations should be limited to investigations of the most serious crimes or the protection of the life of other individuals.

22. National laws should ensure that protections apply strictly, with extremely limited exceptions. Under Belgian law, journalists and editorial staff may be compelled by a judge to disclose information sources only if they are of a nature to prevent crimes that pose a serious threat to the physical integrity of one or more persons, and upon a finding of the following two cumulative conditions: (a) the information is of crucial importance for preventing such crimes; and (b) the information cannot be obtained by any other means. The same conditions apply to investigative measures, such as searches, seizures and telephone tapping, with respect to journalistic sources."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION

37. The applicant complained that the court orders allowing the PGO to access her mobile telephone communications data had constituted an unjustified interference with her right to the protection of journalistic sources. She relied on Article 10 of the Convention, which reads as follows:

"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

38. The Government argued that the complaint was manifestly ill-founded, alleging that the measures of interference complained of had been duly justified under Article 10 § 2 of the Convention.

39. The Court finds that the complaint raises an issue which lends itself to be examined on the merits. It further notes that it is not inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. Submissions by the parties

(a) The applicant

40. The applicant argued that the disputed court orders of 27 August and 18 September 2018, which had allowed the PGO to access her mobile telephone communications data, had constituted an unjustified interference with her rights under Article 10.

41. She considered that the applicable domestic law did not contain sufficient procedural safeguards aimed at the protection of the journalistic sources. In particular, the applicant expressed her dismay with the fact that the order of 27 August 2018 had been taken at an *ex parte* hearing and had not been served on her. If she had not learned of its existence by pure chance, she would never have been able to appeal against it and would not have known that the integrity of her communications data and her sources could be compromised.

42. She further argued that both of the aforementioned court orders had not been necessary in a democratic society.

43. In particular, there had been no pressing social need for the disclosure of the applicant's communications data. Her purported participation in a confidential meeting with S. of the NABU had been a mere "probability". Neither the authenticity of the audio recording of that meeting nor the authenticity of her voice on it had been established with certainty. It had likewise not been established that the PGO officials had exhausted other, more targeted and less intrusive means of establishing the relevant facts. Among other things, they could have started by examining the NABU visitors' log book.

44. The applicant further argued that, in any event, the scope of communications data which could be divulged to the PGO pursuant to the disputed court orders had been grossly disproportionate. In her view, the goal of protecting the reputation of Ms N. or prosecuting the NABU officials for leaking confidential information could not be considered an "overriding interest" for the disclosure of her mobile communications over a

sixteen-month period. This information could lead to the identification of the applicant's sources in journalistic investigations concerning high-profile corruption. The court orders had contained no restrictions concerning the use of this data, making it potentially accessible, at the very least, to the sixteen members of the PGO investigative team working on the case against S. The risk of such disclosure having a detrimental effect had been all the more imminent as at least seven of the applicant's recent investigations concerned corruption within the ranks of the PGO. In addition K., the subject of the NABU investigation in which the information had been leaked, had himself worked at the PGO and could have had an unhealthy interest in the applicant's data.

45. The applicant also pointed out that she had never been able to know with certainty whether either of the judicial orders had been enforced. She submitted that the PGO's written assurances to the contrary (see paragraph 28 above) were not sufficiently convincing. She pointed out that on 4 September 2018 the PGO had in fact asked her mobile telephone operator to disclose the impugned data and that the latter had subsequently refused to inform her whether this request had been satisfied – accordingly, it was not possible to exclude that it had been (see paragraphs 18 and 23 above). Furthermore, it could be discerned from the statements made by the Prosecutor General at a press conference on 15 September 2018 that the operator had in fact responded to the PGO's request (see paragraph 21 above). In any event, even if the two disputed court orders had remained unenforced, this had only been due to the indication of an interim measure by the Court, and not because the domestic authorities had intervened to protect the applicant's rights. She also expressed her fear that the PGO would keep seeking other ways of accessing her communications data, as was evident from the statement by the Prosecutor General himself (see paragraph 26 above).

46. According to the applicant, both the measure of interference authorised by domestic courts and the persistent uncertainty as to whether or not the respective court orders had been enforced and whether the confidentiality of the applicant's sources could be compromised had had a prohibitive chilling effect on her activity as an investigative journalist.

(b) The Government

47. The Government argued that there had been no breach of the applicant's rights under Article 10 in the present case.

48. They submitted the written assurances given by the PGO that neither of the two disputed court orders had been enforced. They also noted that the order of 27 August 2018 had been replaced by the order of 18 September 2018 and the latter had expired on the same date as the District Court's order would have, that is, on 27 September 2018. Therefore, neither of them could still be enforced. Notwithstanding the above, the Government

acknowledged that the aforementioned court orders had amounted to an interference with the applicant's right to impart and receive information under Article 10 of the Convention.

49. The Government argued that the judicial authorisation given to the PGO to access the applicant's communications data in accordance with the provisions of the CCP had been lawful. They further argued that the disputed interference had pursued legitimate aims, in particular, investigation of a serious crime and protection of the rights of Ms N.

50. Access to the applicant's communications data had been necessary to establish the place and date of the meeting during which the NABU officials, in breach of the law, had leaked information protected by the confidentiality of the ongoing criminal investigation and encroaching upon the private life and correspondence of Ms N. Before seeking the disputed authorisation, the PGO officials had exhausted other, less intrusive measures, which could lead to the establishment of the relevant facts crucial for the investigation into the apparent serious crime. In particular, they had questioned the applicant as a witness, but she had refused to provide any information, referring to journalistic privilege against the disclosure of sources.

51. The Government further argued that any shortcomings in the District Court's order of 27 August 2018 (which, according to them, remained unenforced) had been remedied by the order issued by the Court of Appeal on 18 September 2018 to replace it. In particular, the Court of Appeal had taken into account the fact that the applicant was a journalist and was not herself party to the criminal proceedings at issue. It had also restricted the scope of the authorisation to the geolocation data concerning the applicant's presence within a particular perimeter, which had corresponded to the "cell" covering the NABU. The period covered by the authorisation had been limited only to the period of time within which the apparent offence could have been committed. In addition, the authorisation itself could only be enforced during a very limited ten-day period (until 27 September 2018).

52. The Government considered that the applicant's allegations that the disputed measure could result in the identification of her journalistic sources and that her communications data could be used for ulterior motives were unsubstantiated and very general.

(c) The third parties

53. The Media Legal Defence Initiative and Human Rights Platform submitted that the problem of interference with the confidentiality of journalistic sources transcended all member States of the Council of Europe, posing new legal challenges in view of technological advances and the emergence of new types of media, communications and information processing. They suggested that that pre-eminence of the protection of "journalistic sources" in the broadest sense was crucial to the preservation

of the "public watchdog" function of the modern media and that the principles enunciated in Recommendation No. R (2000) 7 (see paragraph 34 above) and the Court's case law remained the guidelines to be followed. The interveners also expressed concern that the Court's judgment in the case of *Becker v. Norway* could be perceived as lowering the source protection standard as compared to the earlier *Tillack v. Belgium* judgment. In particular, it could read as suggesting that the level of source protection might depend on such factors as unscrupulous or illegal conduct of a journalist and, *vice versa*, that a journalist's right to protection of sources might depend on the conduct of a source. In the interveners' view, the appropriate test should not depend on the status of a particular "social communicator", the conduct of such a communicator or the source. Instead, the crucial question should be whether a particular person acted for the purpose of informing the public of a matter of legitimate public interest.

2. The Court's assessment

(a) General principles concerning the protection of journalistic sources

54. The Court reiterates at the outset 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).

55. The Court's understanding of the concept of journalistic "source" covers "any person who provides information to a journalist" and the "information identifying a source" has been considered to include any information likely to lead to the identification of a source, both "the factual circumstances of acquiring information from a source by a journalist" and "the unpublished content of the information provided by a source to a journalist" (see, for example, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, § 86, 22 November 2012 and *Saint-Paul Luxembourg S.A. v. Luxembourg*, no. 26419/10, § 50, 18 April 2013). A chilling effect on the freedom of the press will arise wherever journalists are seen to assist in the identification of anonymous sources (see *Sanoma Uitgevers B.V.*, cited above, § 71).

(b) Application of the above principles in the present case

(i) Whether there was an interference with the applicant's freedom of expression

56. In the present case, the national courts authorised the PGO to access the applicant's communications data stored by her mobile telephone operator. The parties agreed that the impugned authorisation, regardless of whether either of the two relevant court orders had been enforced, had amounted to an "interference" with the applicant's rights under Article 10 of the Convention. The Court sees no reason to hold otherwise.

57. The Court must therefore examine whether the interference was justified under the second paragraph of Article 10 of the Convention, that is, whether it was "prescribed by law", pursued one or more legitimate aims and was "necessary in a democratic society" (see, among other authorities, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, § 141, 27 June 2017).

(ii) Whether the interference was justified

(1) Whether there was "a legitimate aim" for the interference

58. The Court first notes that the aforementioned authorisation was given for the purpose of furthering the investigation concerning the leak of confidential information regarding ongoing criminal proceedings and the private life of Ms N. The Court is therefore satisfied – and it has not been disputed by the parties – that the interference at issue pursued some of the "legitimate aims" listed in Article 10 § 2, in particular, "the prevention of ... crime" and "protection of the reputation or rights of others" (compare *Becker v. Norway*, no. 21272/12, § 60, 5 October 2017).

(2) Whether the interference was "prescribed by law"

59. In considering whether the interference at issue was "prescribed by law", the Court observes that access to the applicant's communications data was authorised by the national judicial authorities under Article 163 of the CCP (see paragraph 31 above). The measure in question therefore had some basis in domestic law. In so far as the applicant complained that the relevant law lacked procedural safeguards, notably as the court decision in her case had been taken at an *ex parte* hearing, it appears that, under the CCP, *ex parte* hearings are only allowed in exceptional cases. Under Article 163 § 2, in order to obtain an *ex parte* hearing, the party who files a request for access to "items and documents" must prove "that there are sufficient grounds to believe that a real threat exists of the items and documents concerned being altered or destroyed". In all other cases, as it appears from Article 163 § 1, the national courts are required to summon the persons concerned by such access requests to the hearings. In the Court's view, this general requirement constitutes an important procedural

safeguard for all persons potentially concerned by data access requests, including journalists.

60. It appears that in the applicant's case, this safeguard was not implemented owing to the particular interpretation of Article 163 of the CCP by the District Court. Rather than enunciating specific reasons for considering the PGO's request without summoning the applicant, the District Court made a formulaic reference to the "threat of the information sought being altered or destroyed" (see paragraph 16 above). In the Court's view, giving more ample reasons for justifying the above finding was of significant importance, in particular, because the data in question, stored by the applicant's mobile operator, was not in her personal possession. As a consequence of the District Court's decision to apply Article 163 § 2, the applicant was also not notified by it that the PGO had obtained an authorisation to access her communications data and, once she learned about that authorisation from other sources, the District Court refused to provide her with a copy of its respective order (see paragraphs 17 and 19 above). It appears that had it not been for a pure chance that the applicant became aware of that order, she might not have been able to make use of any procedural safeguards existing in the domestic law for protecting her rights. The Court is deeply concerned with this possibility, which would be tantamount to arbitrariness. However, given that in this particular case, the applicant did in fact learn about the existence of the disputed order and the Court of Appeal found it possible to accept her appeal for consideration and to quash the order, the Court finds that the crux of the applicant's remaining argument before it concerns the relevance and sufficiency of the reasons provided by the judicial authorities for authorising the interference with her protected data. The Court therefore finds it necessary to continue its examination of the case by turning to the question whether the interference was necessary in a democratic society (compare *Nagla v. Latvia*, no. 73469/10, §§ 87-91, 16 July 2013; and *Becker*, cited above, §§ 63-64).

(3) Whether the interference was "necessary in a democratic society"

– *General principles*

61. The Court reiterates that its task in assessing the "necessity" of the interference is not to take the place of the national authorities, but rather to review, in the light of the case as a whole, whether the decisions they have taken pursuant to their power of appreciation were compatible with the provisions of the Convention relied upon (see, among other authorities, *Telegraaf Media Nederland Landelijke Media B.V. and Others*, cited above, § 124). The Court must accordingly examine the reasons given by the judicial authorities for authorising access to information together with the scope of that access, in order to ascertain whether those reasons were "relevant" and "sufficient" and thus whether, having regard to the

margin of appreciation afforded to the national authorities, the interference was proportionate to the legitimate aims pursued and whether it corresponded to a "pressing social need" (see, among other authorities, *Nagla*, cited above, § 94).

62. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society, the Court has repeatedly stated that limitations on the confidentiality of journalistic sources call for the most careful scrutiny (see, among other authorities, *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 46, ECHR 2003-IV, and *Saint-Paul Luxembourg S.A.*, cited above, § 58). An interference potentially leading to disclosure of a source cannot be considered "necessary" under Article 10 § 2 unless it is justified by an overriding requirement in the public interest (see, among other authorities, *Roemen and Schmit*, cited above, § 46; *Voskuil v. the Netherlands*, no. 64752/01, § 65, 22 November 2007; and *Becker*, cited above, §§ 65-66, with further references). The Court has previously held that to establish the existence of an "overriding requirement" it may not be sufficient for a party seeking disclosure of a source to show merely that he or she will be unable without disclosure to exercise the legal right or avert the threatened legal wrong on which he or she bases the claim: the considerations to be taken into account by the Court for its review under Article 10 § 2 tip the balance of competing interests in favour of the interest of democratic society in securing a free press (see *Goodwin*, cited above, § 45; compare also *Roemen and Schmit*, cited above, § 58; *Voskuil*, cited above, § 72; *Martin and Others v. France*, no. 30002/08, § 87, 12 April 2012; and *Ressiot and Others v. France*, nos. 15054/07 and 15066/07, § 126, 28 June 2012). In this connection, the right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources, but is part and parcel of the right to information, to be treated with the utmost caution (see, among other authorities, *Tillack v. Belgium*, no. 20477/05, § 65, 27 November 2007).

63. In a series of cases concerning searches of journalists' homes and workplaces and the seizure of journalistic material, the Court recognised that such measures, even if unproductive, constituted a more drastic type of interference than a targeted order to divulge the source's identity, since such measures had allowed the relevant authority to obtain access to a broad range of the material used by the journalists in discharging their professional functions (see, among other authorities, *Roemen and Schmit*, cited above, § 57; *Ernst and Others v. Belgium*, no. 33400/96, § 103, 15 July 2003; *Nagla*, cited above, § 95; and *Görmüş and Others v. Turkey*, no. 49085/07, § 73, 19 January 2016). Similar conclusions were reached by the Court in a case where the seizure also concerned, among other things, the journalists' communications data (see *Ressiot and Others*, cited above, § 125).

– *Application of those principles in the present case*

64. Examining the present case in the light of the aforementioned principles, the Court considers that the reasons given by the domestic judicial authorities for the interference with the applicant's rights under Article 10 were not sufficient to demonstrate that the interference was proportionate and that it corresponded to a pressing social need.

65. In this connection, the Court notes firstly that the District Court's order of 27 August 2018 authorised the PGO to collect a wide range of the applicant's protected communications data concerning her personal and professional contacts over a sixteen-month period. The disputed authorisation included, in particular, access to information concerning the time and duration of the applicant's communications and the telephone numbers of her contacts (see paragraphs 15-16 above). This data could possibly include identifiable information concerning the applicant's confidential sources which had no relevance to the criminal proceedings regarding the alleged misconduct of S. (compare and contrast *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 151, ECHR 2006-XI). The risk of detriment to the interests protected by Article 10 was all the greater as the focus of the applicant's work as a journalist had been on investigating high-profile corruption, including corruption within the PGO itself. The District Court's order contained no safeguards excluding the possibility that information potentially leading to the identification of any such sources would become available to a wide circle of PGO officials and could be used for purposes unrelated to the criminal investigation concerning S. These elements are sufficient for the Court to conclude that the scope of the data access authorisation in the court order of 27 August 2018 was grossly disproportionate to the legitimate aims of investigating a purported leak of classified information by S. and protecting Ms N.'s private life.

66. The Government argued that the flaws in the District Court's order had been rectified since the Court of Appeal had accepted the applicant's appeal for consideration and had quashed that order, which remained unenforced. However, the Court considers that the first order nevertheless provides relevant and important context in the present case.

67. It notes in this respect that the wording of the aforementioned order indicated that it was not amenable to appeal. Notwithstanding that on 18 September 2018 the Court of Appeal quashed it, having exceptionally accepted the applicant's appeal for consideration, between 27 August and 18 September 2018 the order was considered final and enforceable. It is evident from the case file that the PGO made at least one attempt, namely, on 4 September 2018, to collect some of the applicant's data with reference to the order in question (see paragraph 18 above). Subsequently, the PGO officials gave inconclusive information as to whether or not the applicant's mobile operator had responded to that letter and whether it had divulged any of the applicant's data.

68. For instance, on 15 September 2018, the Prosecutor General indicated at a press-conference that he was, in principle, ready to show the reply from the mobile operator to reassure the applicant and the public that no data identifying any journalistic sources had been received by the PGO (see paragraph 21 above). His statement created an appearance that the PGO had obtained some sort of communication from the mobile operator and that that communication could be accessed by those interested. However, on 20 September 2018 the PGO refused to provide either the aforementioned reply purportedly received from the operator, or any information as to whether or not any such reply had been received (see paragraph 23 above). Next, on 27 September 2018, in his interview at the Parliament, the Prosecutor General denied having received any reply from the mobile operator (see paragraph 26 above). Finally, on 12 February 2019 the PGO indicated to the Government's Agent, within the framework of the present proceedings, that, overall, they had not carried out any actions authorised by either of the two disputed court orders (see paragraph 28 above). Based on the aforementioned submissions viewed in the light of other available material, the Court is unable to draw a definite conclusion as to whether or not the integrity of the applicant's communications data was preserved during the period of validity of the District Court's order.

69. The Court agrees that the new data access authorisation given on 18 September 2018 by the Court of Appeal, which replaced the District Court's authorisation and was limited essentially to the collection of her geolocation data over a sixteen-month period, could remove the aforementioned threat of identification of the applicant's sources unrelated to the proceedings against S., assuming that the PGO had not previously received any such data from the applicant's mobile operator, as alleged by the Government. However, it is notable that S. was himself treated by the PGO authorities as the applicant's journalistic source. They sought access to the applicant's data precisely to test an assumption that S. had met with the applicant in order to provide her with confidential information relevant to her activity as an investigative journalist and, if so, to use her data as evidence in criminal proceedings against him. The fact that the name of the applicant's purported source was known to the authorities and that he was implicated in a criminal offence did not as such remove the applicant's own protection under Article 10 of the Convention (compare *Nagla*, § 95, and *Becker*, §§ 72 and 82, both cited above).

70. Accordingly, for the purposes of Article 10 of the Convention, the Court of Appeal was still bound to demonstrate that the seizure of her geolocation data was justified by an overriding requirement in the public interest. In other words, the Court of Appeal had to indicate why the interest in obtaining the applicant's geolocation data sought by the PGO was of a vital nature for combatting serious crime; to ascertain that there were no reasonable alternative measures for obtaining the information sought by the

PGO; and to demonstrate that the legitimate interest in the disclosure clearly outweighed the public interest in the non-disclosure (compare *Goodwin*, § 45, and *Ressiot and Others*, §§ 122 and 126, both cited above).

71. The Court finds that the text of the Court of Appeal's ruling did not sufficiently respond to these requirements. Firstly, this ruling authorised access to the applicant's protected geolocation data over a sixteen-month period. In view of the length of that period and the size of the geographical area of the city centre of Kyiv in respect of which the geolocation data was sought[1], the applicant's telephone could have been registered there on a number of occasions which had no relevance to the case under investigation by the PGO. Secondly, by way of justifying the pressing social need for the interference with the applicant's rights, the Court of Appeal referred only to the purpose of "achieving efficiency" in a criminal investigation and establishing "more exactly the time and place" of the purported confidential meeting (see paragraph 22 above) without providing any indication why these considerations outweighed the public interest in non-disclosure of the applicant's protected geolocation data. Thirdly, based on the case file, at the relevant time there remained considerable uncertainty that any information pertinent to the proceedings against S. would be retrieved from the applicant's communications data. It appears from the material in the Court's possession that at the relevant time it had not been unequivocally established that S.'s alleged meeting with the journalists had been held on the NABU's premises or some other premises located within the geographical area targeted by the PGO for the collection of the applicant's geolocation data, or that the applicant had indeed been a participant in the meeting. Even so, the applicant might not have necessarily had her telephone with her at the time. Fourthly, it does not appear that the Court of Appeal delved into the question whether there were other more targeted means of obtaining the information which the investigative authority had hoped to retrieve from the applicant's communications data.

72. In view of the above considerations, the Court is not convinced that the data access authorisation given by the domestic courts was justified by an "overriding requirement in the public interest" and, therefore, necessary in a democratic society (see *Goodwin*, cited above, § 45; *Voskuil*, cited above, § 72; and *Becker*, cited above, § 83).

73. There has accordingly been a breach of Article 10 of the Convention in the present case.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

74. The applicant also argued that the same considerations as those which she had mentioned in respect of Article 10 also gave basis for finding

[1] According to the maps, Povitroflotskiy Avenue alone extends for over six kilometres

a violation of Article 13 of the Convention concerning the absence of effective remedies for her complaints under Article 10.

75. The Government argued that there had been no breach of Article 13 in the present case. They submitted that while the data access authorisation issued by the District Court had been too broad, the applicant had been able to have it quashed on appeal.

76. The Court considers that in view of its relevant findings under Article 10 of the Convention, it is not necessary to address this complaint in the present case.

III. RULE 39 OF THE RULES OF COURT

77. Regard being had that the authorisation to access the applicant's communications data given by the domestic courts to the PGO has expired, the Court considers that it is appropriate to discontinue the interim measure indicated to the Government under Rule 39 of the Rules of Court (see *Konovalchuk v. Ukraine*, no. 31928/15, § 100, 13 October 2016).

IV. APPLICATION OF ARTICLE 41 OF THE CONVENTION

78. 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

79. The applicant claimed EUR 10,000 euros (EUR) in respect of non-pecuniary damage.

80. The Government submitted that the applicant's claim for damage was unsubstantiated.

81. The Court, ruling on an equitable basis, awards the applicant EUR 4,500 in respect of non-pecuniary damage, plus any tax that may be chargeable.

B. Costs and expenses

82. The applicant also claimed EUR 2,350 for the costs and expenses incurred before the Court, comprising legal fees of EUR 1,400 and EUR 950 for her representation by Mr S. Zayets and Ms L. Pankratova respectively. The applicant provided time sheets stating that her representatives spent 14 and 9.5 hours on working on the present case and each charged EUR 100 per hour.

83. The Government submitted that the applicant's claim was not supported by the appropriate documents. In particular, she had not provided copies of legal services contracts with Mr Zayets and Ms Pankratova.

84. 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 above criteria and the documents in the Court's possession, the Court considers it reasonable to award the applicant EUR 2,350 for legal fees, plus any tax that may be chargeable on that amount.

C. Default interest

85. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

V. ARTICLE 46 OF THE CONVENTION

86. The applicant also asked the Court to indicate to the Government, under Article 46 of the Convention, to implement general measures addressing the protection of journalistic sources, for example, by amending legislation. The applicant did not make any further concrete proposals in this regard.

87. The Government argued that the Ukrainian legislation had sufficient safeguards for the protection of journalistic sources and there was no need for amending it.

88. The Court points out that by Article 46 of the Convention the High Contracting Parties undertook to abide by the final judgments of the Court in any case to which they were parties, execution being supervised by the Committee of Ministers. It follows, *inter alia*, that a judgment in which the Court finds a breach of the Convention imposes on the respondent State a legal obligation not just to pay those concerned the sums awarded by way of just satisfaction, but also to choose, subject to supervision by the Committee of Ministers, appropriate individual measures to fulfil its obligations to secure the rights of an applicant (see *Magnitskiy and Others v. Russia*, nos. 32631/09 and 53799/12, § 294, 27 August 2019, with further references).

89. The Court reiterates that its judgments are essentially declaratory in nature and that, in general, it is primarily for the State concerned to choose, subject to supervision by the Committee of Ministers, the means to be used in its domestic legal order in order to discharge its obligation under Article 46 of the Convention, provided that such means are compatible with the conclusions set out in the Court's judgment (ibid., § 295).

90. Only exceptionally, with a view to helping the respondent State to fulfil its obligations under Article 46, will the Court seek to indicate the type of measure that might be taken in order to put an end to a violation it has found (ibid., § 296).

91. Regard being had to the circumstances of the present case and the submissions by the parties, the Court does not consider it necessary to indicate any individual or general measures that the State has to adopt for the execution of the present judgment.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the complaint under Article 10 of the Convention admissible;

2. *Holds* that there has been a violation of Article 10 of the Convention;

3. *Holds* that it is not necessary to examine the complaint under Article 13 of the Convention;

4. *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 4,500 (four thousand five hundred euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
      (ii) EUR 2,350 (two thousand three hundred and fifty euros), plus any tax that may be chargeable to the applicant, in respect of legal fees;
   (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;

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

Done in English, and notified in writing on 1 April 2021, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Victor Soloveytchik
Registrar

Síofra O'Leary
President