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

FIFTH SECTION

DECISION

Application no. 27237/19
KYIVSTAR, PAT
against Ukraine

The European Court of Human Rights (Fifth Section), sitting on 16 January 2024 as a Chamber composed of:

Georges Ravarani*, President*,
Lado Chanturia,
Mārtiņš Mits,
Stéphanie Mourou-Vikström,
María Elósegui,
Kateřina Šimáčková,
Mykola Gnatovskyy*, judges*,
and Victor Soloveytchik, *Section Registrar,*

Having regard to the above application lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Ukrainian joint-stock company, Kyivstar, PAT ("the applicant company") on 15 May 2019,

Having regard to the decision to give notice of the application to the Ukrainian Government ("the Government"),

Having regard to the parties' observations,

Having deliberated, decides as follows:

THE FACTS

1. The applicant company, established in 1997, was represented by Mr Y. Kotliarov, a lawyer practising in Kyiv.

2. The Government were represented by their Agent, Ms M. Sokorenko, of the Ministry of Justice.

3. On 7 April 2017 the Antimonopoly Committee ("the AC") asked the applicant company to provide, within ten calendar days, information about the mobile telephone communications of two individuals between January and May 2015. In particular, the information requested was to include any

telephone numbers which those individuals had used, any telephone numbers they had dialled or received calls from, and the relevant dates, times and duration of the calls. The AC needed the information to investigate a possible breach of competition regulations by two private companies which those individuals had represented when they were bidding in public procurement tendering process in May 2015. The AC had made its requests with reference to a specific telephone number ending with 71 which it believed belonged to one of the individuals concerned.

4. By a letter of 13 April 2017, the applicant company replied that the data requested had no relation to the investigation referred to by the AC. The applicant company said that it could only have provided the data if the AC had demonstrated that the data had been necessary for the exercise of its statutory functions or if a request had been made in accordance with the procedure set out in Chapter 15 of the Code of Criminal Procedure (see paragraph 22 below).

5. On 26 June 2017 the AC instituted proceedings against the applicant company under section 50 of the Protection of Economic Competition Act of 2001 (see paragraph 24 below) because it had failed to provide the data requested, and it informed the applicant company accordingly.

6. On 20 July 2017 the AC asked the applicant company to provide the communications data previously requested on 7 April 2017 and, in addition to that, to provide information about any communications between January and May 2015 involving the specific telephone number ending with 71. The AC specified that the telephone number had been referred to by one of the individuals who featured in the tender documents (see paragraph 3 above).

7. On 5 August 2017 the applicant company replied to the AC that the two individuals concerned had not been registered as subscribers of its telecommunications services during the period in question. The specific telephone number indicated in the AC's request had been used anonymously for a telephone operated on a "pay-as-you-go" basis, which did not require subscription. Under Article 159 of the Code of Criminal Procedure, communications data relating to that telephone number could not be disclosed because there was no written consent by the user concerned (see paragraph 22 below).

8. On 15 September 2017 the AC sent the applicant company its "preliminary conclusion" that, by continuing to fail to provide the information first requested on 7 April 017, the applicant company had committed a breach of point 13 of section 50 of the Protection of Economic Competition Act of 2001 (see paragraph 24 below).

9. On 20 September 2017 the applicant company sent a letter to the AC challenging its above-mentioned "preliminary conclusion" (see paragraph 8 above).

10. On 23 November 2017 the AC determined that the applicant company should pay a fine of 54,400 Ukrainian hryvnias (the equivalent of approximately 1,700 euros at the time) for having failed to provide the information that the AC had requested on 7 April 2017.

11. In a letter of 26 December 2017 addressed to the applicant company, the Ukrainian Association of Communications Operators *TELAS* (*ТЕЛАС*) expressed the view that the AC "had exceeded its powers when requiring the provision of confidential information about telephone communications without the customers' consent".

12. On 24 January 2018 the Head of the Secretariat of the Parliamentary Commissioner for Human Rights, in reply to a letter of 12 December 2017 from the applicant company, informed it, *inter alia*, that there existed "a systemic problem of a lack of clarity in the legal regulation of the power of certain State bodies, notably the Antimonopoly Committee, to access personal data in the context of the exercise of their functions, which created a basis for systematic abuse [of that power] and excessive interference with the right to privacy". The Head of the Secretariat cited Articles 31 and 32 of the Constitution; Article 159, Article 162 § 1(7) and Article 163 § 6 of the Code of Criminal Procedure; sections 7, 17, 22 and 22-1 of the Antimonopoly Committee Act of 1993; section 34 of the Telecommunications Act of 2003; sections 14, 16 and 23 of the Personal Data Protection Act of 2010; and sections 42 and 47 of the Regulations on Telecommunications Services enacted by the Cabinet of Ministers on 11 April 2012 (see paragraphs 20-30 below). Referring to sections 10(3), 14(3), 16 and 24(1) of the Personal Data Protection Act of 2010, the Head of the Secretariat drew the applicant company's attention to the fact that the holders of personal data bore an obligation to protect those data.

13. On 25 January 2018 the applicant company lodged a claim challenging the AC's decision of 23 November 2017 in the Kyiv Commercial Court. The applicant company argued principally that its refusal to provide the AC with confidential information about telecommunications services as requested had been lawful. The applicant company could only have provided that information with the users' consent or pursuant to a court order. It also argued that the AC had requested information which potentially concerned other users with whom the individuals identified in the request could have communicated. The applicant company argued that judicial practice regarding breaches of competition regulations did not require information about suspects' communications to be produced in evidence and, in any event, information about the communications of an anonymous user (see paragraph 7 above) would be of no evidential value. The applicant company submitted that, in the past, the AC had generally agreed that such information could not be disclosed without the users' consent or a court order.

14. On 11 June 2018 the Kyiv Commercial Court found for the applicant company. Relying mainly on Articles 31 and 32 of the Constitution and Article 15 § 2, Article 162 § 1(7) and Article 163 of the Code of Criminal Procedure (see paragraphs 20-22 below), the court held that the AC had no power to require disclosure of personal communications data without the users' consent or a court order.

15. On 4 September 2018 the Kyiv Commercial Court of Appeal upheld the Commercial Court's judgment of 11 June 2018.

16. On 26 September 2018 the AC lodged an appeal on points of law with the Supreme Court.

17. On 20 November 2018 the Supreme Court found for the AC and quashed the lower courts' decisions. The Supreme Court found *inter alia* that the AC had acted in accordance with Article 32 of the Constitution, section 22-1 of the Antimonopoly Committee Act of 1993; sections 50 and 52 of the Protection of Economic Competition Act of 2001; and section 34 of the Telecommunications Act of 2003 (see paragraphs 20 and 23-25 below) and had not violated Article 8 of the Convention. The AC's actions had been necessary in the public interest in preventing, investigating and terminating breaches of competition regulations, since it had not been able to obtain the data requested by any other means.

18. The Supreme Court also noted that the data requested were of a technical nature and did not concern the content of the communications. No court order had therefore been necessary under Article 31 of the Constitution (see paragraph 20 below).

19. Lastly, the Supreme Court held that the provisions of the Code of Criminal Procedure had been inapplicable in the present case.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. CONSTITUTION OF UKRAINE

20. The relevant provisions of the Constitution read as follows:

Article 31

"Everyone shall be guaranteed secrecy for their mail, telephone conversations, telegraph and other correspondence (*Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції*). Exceptions shall be established only by a court where provided for by law, with the purpose of preventing crime or ascertaining the truth in the course of the investigation of a criminal case, if it is not possible to obtain the information by other means."

Article 32

"No one shall be subject to interference in their personal and family life, except where provided for by the Constitution of Ukraine.

> The collection, retention, use and dissemination of confidential information about a person without their consent shall not be permitted, except where determined by law and only in the interests of national security, economic welfare and human rights.
>
> ..."

II. CODE OF CRIMINAL PROCEDURE

21. Article 15 of the Code of Criminal Procedure makes the protection of private life one of the fundamental principles of criminal proceedings. No one may collect, store, use or disseminate information about the private life of any person without that person's consent, except where provided for by the Code. Such information cannot be used other than for the purposes of criminal proceedings. Those who are given access to such information are obliged to prevent its disclosure.

22. Chapter 15 sets out rules for temporary access to objects and documents, including information about telecommunications (Article 162 § 1(7)) that may be given by those possessing such objects or documents to a party to criminal proceedings, pursuant to a court order (Article 159). In particular, an investigating judge or a court may order temporary access to such information if the party applying for access has shown that it would be of evidential value in criminal proceedings and that it is impossible to use other evidence instead (Article 163 § 6).

III. ANTIMONOPOLY COMMITTEE ACT OF 1993

23. Section 1 of the Antimonopoly Committee Act of 1993 provides that the AC is a special State body with the role of ensuring "State protection of competition in business and public procurement". To that end, the AC, its staff and its divisions may, *inter alia*, investigate and determine cases concerning alleged breaches of competition law, in the course of which they are empowered to issue directions for legal entities and individuals to provide information, including that to which access is restricted, if it is "needed to fulfil the tasks set out in the legislation on the protection of economic competition" (sections 7, 16, 17, 22 and 22-1). Such information must be used "exclusively" to ensure the fulfilment of those tasks and may not be disclosed except in cases specifically provided for by law (section 22-1).

IV. THE PROTECTION OF ECONOMIC COMPETITION ACT OF 2001

24. Under sections 50 and 52 of the Protection of Economic Competition Act of 2001, a failure to provide information requested by the AC, a member of its staff or a territorial branch within the set time-limit and the provision of incomplete information constitute a breach of "the legislation on the protection of economic competition" punishable by a fine of up to 1% of the entity's income for the year preceding that in which the fine is imposed.

V. TELECOMMUNICATIONS ACT OF 2003

25. Section 34 of the Telecommunications Act of 2003 obliges telecommunications providers to ensure the "preservation" of information about the telecommunications services provided to their users. Such information can be disclosed without the users' consent where that is provided for by law.

VI. PERSONAL DATA PROTECTION ACT OF 2010

26. Under Section 2 of the Personal Data Protection Act of 2010, "personal data" includes "information about an identified or identifiable physical person". Section 5 provides that personal data can be designated as confidential by law or by the person concerned. However, data concerning the performance of the functions of public officials cannot be designated as confidential. Sections 6 and 14 permit disclosure of personal data without the person's consent in cases provided for by law and in the interests of national security, economic welfare or human rights. Processing of data in a form enabling the identification of the person concerned further than is justified by a lawful aim is prohibited. Those who share and obtain personal data, including the employees and retired staff of communications service providers, are responsible for ensuring the confidentiality of such data (sections 10(3), 14(3) and (4) and 24(1)). The law may impose an obligation on those who retain personal data to process them without the person's consent (section 11). Those who process data which entails "a risk for the rights and freedoms" of the person concerned must inform the Parliamentary Commissioner for Human Rights, who is responsible for ensuring that personal data protection legislation is observed (sections 22 and 23). Pursuant to section 15, personal data must be deleted or destroyed when, *inter alia*, the term for their retention has expired or pursuant to an order of a court or of the Parliamentary Commissioner for Human Rights or of officials of the Secretariat of the Commissioner designated by him or her.

27. Under section 16, the procedure for obtaining access to personal data is determined by the terms of the consent to personal data processing given by the person concerned or by law. A request for access to personal data must specify, *inter alia*, the data requested, the identity of the person concerned and the purpose of or grounds for the request. The holder of the data must examine the request within ten working days and inform the person seeking the data whether access will be granted or not. The information requested must be provided within thirty days.

28. Under section 21, the person concerned does not have to be notified of the transfer of his or her data in cases involving the public authorities' "exercise of statutory powers".

29. Section 8 guarantees everyone the right to challenge the processing of his or her personal data in the courts or with the Parliamentary Commissioner for Human Rights. The Commissioner has the power, *inter alia*, to monitor the processing of personal data by any person who holds them and to give directions in that regard, including to cease the processing of personal data and to give or refuse access to them.

VII. REGULATIONS ON TELECOMMUNICATIONS SERVICES ENACTED BY THE DECREE OF THE CABINET OF MINISTERS OF 11 APRIL 2012

30. Pursuant to section 39 of the Regulations on Telecommunications Services enacted by the Cabinet of Ministers on 11 April 2012, telecommunications service providers (operators) are obliged to keep records of the services provided and their cost during the limitation period for civil claims relating to disputes arising out of contractual relations with their clients. Telecommunications service providers (operators) are also obliged "to take measures in accordance with the law to ensure that telephone communications and other information transferred through telecommunications networks are kept secret and to protect customer information collected when concluding contracts or providing services and other information to which access is restricted". Sections 42 and 43 require telecommunications service providers (operators) to keep and preserve such information, to create databases for that purpose and not to disclose "information to which access is restricted". Information about the services provided must be given to customers. It may also be given to others in accordance with the users' written consent or pursuant to law (sections 45, 49 and 51). Section 47 prohibits the disclosure of information about customers' locations without their consent except where otherwise provided for by law.

VIII. JUDGMENT OF THE CONSTITUTIONAL COURT OF UKRAINE OF 20 JANUARY 2012

31. In its judgment of 20 January 2012 the Constitutional Court gave the official interpretation of Articles 32 and 34 of the Constitution, which guarantee the rights to respect for private life and to freedom of speech respectively.

32. The court held that all information about private and family life was confidential but that information about public officials' performance of their functions was not. Confidential information included all information about relations of a monetary and non-monetary nature, events, matters associated with a person and his or her family – information about ethnicity, education, civil status, religious beliefs, health, property, address, date and place of birth, and information about events in the day-to-day, intimate, professional,

business and other spheres of the person's life. The collection, retention, use and dissemination of such information without the person's consent was permitted only in cases provided for by law in the interests of national security, economic welfare or human rights.

IX. DOMESTIC CASE-LAW CITED BY THE GOVERNMENT

33. In their observations in the present case, the Government referred to five judgments given by the Supreme Court between February 2018 and January 2020 in cases in which private banks had challenged fines imposed by the AC for their failure to provide it with certain banking information about their clients which it had needed to investigate violations of competition law. The banks' claims had been dismissed mainly because compliance with the AC's requests for information had been compulsory pursuant to sections 7, 16, 17, 22 and 22-1 of the Antimonopoly Committee Act of 1993 (see paragraph 23 above), which were *lex specialis* in relation to the regulations on access to secret bank data.

34. The Government also cited the Supreme Court's judgment of 18 February 2020 in a case in which a private company had challenged a finding of the AC that it had been involved in a cartel in the course of a public procurement procedure. The Supreme Court found, *inter alia*, that information about the IP address used by all the bidders in the procurement procedure – which had been obtained pursuant to sections 17 and 22-1 of the Antimonopoly Committee Act of 1993 – had been lawfully admitted as one of the key pieces of evidence in the case despite the company's argument that it had not been obtained in accordance with the Code of Criminal Procedure or the Telecommunications Act of 2003. In that context, the provisions of the Antimonopoly Committee Act of 1993 were *lex specialis* in relation to the provisions of the Criminal Procedure Code and the Telecommunications Act of 2003 (see paragraphs 22, 23 and 25 above).

X. CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

35. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), opened for signature on 28 January 1981, entered into force in respect of Ukraine on 1 January 2011. The relevant parts of this convention read as follows:

Article 2 – Definitions

"For the purposes of this Convention:

(a) 'personal data' means any information relating to an identified or identifiable individual ('data subject');

...

(c) 'automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

..."

Article 5 – Quality of data

"Personal data undergoing automatic processing shall be ...

(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

...

(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

COMPLAINTS

36. The applicant company complained that, by requiring it to provide confidential telecommunications information about users of its services and by imposing a fine on it for refusing to do so, the authorities had violated Article 8 of the Convention. The applicant company also complained about a violation of Article 10 of the Convention and Article 1 of Protocol No. 1 on that account.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

A. The parties' submissions

1. The Government

37. The Government submitted that the applicant company's complaint had to be rejected as incompatible *ratione personae* with the provisions of the Convention. In their view, the applicant company could not claim to be a victim of the alleged violation of Article 8, since the information requested had concerned the communications of two individuals and not of the applicant company and consequently it had suffered no damage or disadvantage.

38. They further argued that the complaint was groundless. In particular, the AC had acted within its powers, on the basis of sufficiently accessible and foreseeable legal provisions, in order to obtain information essential for the investigation of a suspected breach of competition law. The AC's request was

limited in its scope to technical data concerning the communications of two individuals and did not concern their content. The applicant company had been able to challenge the AC's actions and decisions ultimately in the Supreme Court, which had given a decision which was duly reasoned and consistent with its practice in similar cases (see paragraphs 33-34 above).

2. The applicant company

39. The applicant company contended that it had been the victim of the alleged violation of Article 8 given that it had been legally obliged to protect the telecommunications data of users of its services and had been fined for having refused to provide that data to the authorities. Furthermore, compelling the applicant company to provide the data in question to the authorities could have had a negative impact on its business reputation and consequently on its goodwill.

40. The applicant company also argued that the AC's request for them to provide the data in question had been made without a valid reason, in breach of Articles 159 and 163 of the Code of Criminal Procedure (see paragraph 22 above). Section 22-1 of the Antimonopoly Committee Act of 1993 and section 34 of the Telecommunications Act of 2003 (see paragraphs 23 and 25 above), on which the request was based, permitted disclosure of telecommunications data without notifying the users concerned and without giving them an opportunity to challenge the disclosure and thus were contrary to Article 8 of the Convention. The Antimonopoly Committee Act of 1993 was also in contravention of Articles 31 and 32 of the Constitution and the Code of Criminal Procedure (see paragraphs 20, 22 and 23 above), which had higher legal force and required prior judicial authorisation or the consent of the persons concerned to access private communications data. The applicant company referred to the letter of 24 January 2018 from the Secretariat of the Parliamentary Commissioner for Human Rights pointing to a lack of clarity in the regulations giving the AC power to access personal data, which created the potential for the systematic abuse of and excessive interference with the private life of individuals (see paragraph 12 above). The decisions of the Supreme Court to which the Government had referred were allegedly irrelevant to the present case, since they did not concern the disclosure of the telecommunications data of an unspecified number of users (see paragraphs 33-34 above).

41. The applicant company submitted that the relevant domestic law did not provide for *ex-post facto* judicial review of the AC's requests to provide information, which created a high risk of abuse of those powers. The Supreme Court's review of the present case had been "rather formalistic" and had not addressed the questions of the lawfulness and necessity of the interference complained of. The court had disregarded the fact that the data requested were an integral part of the users' telecommunications and concerned their rights and interests and those of the applicant company.

42. The applicant company alleged that the AC could not be regarded as a "fully independent and impartial" body since it was headed by a State Commissioner who was appointed by the President on a proposal by the Prime Minister.

43. There was also a possibility that after having obtained the requested data the AC would disclose it to the law-enforcement authorities, thereby circumventing the procedure of prior judicial authorisation specified by the Criminal Procedure Code (see paragraph 22 above).

44. Under section 7 of the Antimonopoly Committee Act of 1993 (see paragraph 23 above), the AC could have asked the law-enforcement authorities to obtain any information necessary for its investigation through the procedure provided for in the Code of Criminal Procedure.

45. The AC's request in the present case had not complied with the requirements set out in Article 5 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (see paragraph 35 above) in that the AC had not explained why it was necessary to disclose all incoming and outgoing calls potentially involving a large number of users.

46. Lastly, there was no time-limit on the storage of data obtained by the AC.

B. The Court's assessment

47. At the outset, the Court notes that, in its letter of 5 August 2017 to the AC, the applicant company clarified that the two individuals whose communications data had been requested by the AC had not been among its subscribers during the period in question (see paragraphs 3 and 7 above). It therefore appears that the applicant company effectively provided, albeit with a delay, all the information it possessed in that regard, as requested by the AC in respect of the two named individuals. At the same time, the applicant company did not deny that it operated the telephone number ending with 71 which the AC believed had been used by one of the investigated individuals but refused to disclose the information concerning that number despite the AC's request.

48. In the light of the foregoing and the applicant company's specific submissions, while it is true that the impugned decision to impose a fine apparently did not make the above distinction, the Court considers that the scope of the present complaints is essentially limited to the imposition of a legal obligation on the applicant company to disclose information about telephone calls made to and from the anonymous telephone number specified in the AC's requests (see paragraphs 3 and 6 above) and the imposition of a fine for its failure to do so.

49. The Court further notes that the Government's argument that the applicant company could not claim to be a victim of a violation of Article 8 on account of the events complained of is closely linked to the question of that provision's applicability *ratione materiae* to the circumstances of the present case (see paragraphs 37 and 39 above). The question may arise in this context as to whether the impugned obligation imposed by the authorities, which was limited to providing a list of telephone numbers from which or to which calls were made during a specified period to or from one anonymous telephone number operated by the applicant company, and the fine imposed on it for failure to provide this limited type of information, concerned the Article 8 rights of the applicant company, seeing that its own communications were not at stake. The Court does not need to resolve these questions, however, because, even assuming that Article 8 applies, the applicant company's complaints should be declared inadmissible as being manifestly ill-founded for the reasons set out below.

50. Firstly, the Court finds that there was sufficient legal basis for requiring the applicant company to provide the AC with the telecommunications data requested and for imposing a fine on it for refusing to do so.

51. In particular, the AC's actions challenged by the applicant company were mainly based on Article 32 of the Constitution, sections 7, 16, 17, 22 and 22-1 of the Antimonopoly Committee Act of 1993 and Sections 50 and 52 of the Protection of Economic Competition Act of 2001, which were accessible to the public and sufficiently clear and foreseeable in their consequences. Regard being had to the interpretation of those provisions by the Supreme Court in the present case, which does not appear to be arbitrary or manifestly unreasonable, and also in other cases referred to by the Government, the AC had the power to oblige physical and legal persons to provide it with various types of information, including the telecommunications data in question, which it needed for its investigation of alleged breaches of competition law, and it also had the power to apply financial sanctions for not complying with its requests (see paragraphs 17-20, 23, 24, 33 and 34 above). Contrary to the applicant company's submissions, it transpires from the Supreme Court's case-law that no court order was necessary under Article 31 of the Constitution in the present case and that the Code of Criminal Procedure did not apply either (ibid.). The applicable domestic law therefore did not require a prior judicial authorisation in the particular circumstances.

52. It is true that the Head of the Secretariat of the Parliamentary Commissioner for Human Rights' letter of 24 January 2019 stated, in very general terms, that there was a "systematic problem of a lack of clarity" in the relevant legislative provisions and consequently a basis for "systemic abuse" of the AC's powers, but the Court observes that this statement was not supported with further explanation or concrete examples (see paragraph 12

above). As the Court has already found above, the manner in which the relevant legal provisions were applied in the present case involved no ambiguity or arbitrariness (see paragraph 51 above). The AC used its statutory powers to compel the applicant company to provide telecommunications data that was clearly defined and limited in scope and which the AC believed could contain evidence of a breach of competition regulations in the course of a public procurement process (see paragraphs 3, 6, 8 and 10 above). Also, the applicant company's allegation that the AC acted in breach of Article 5 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (see paragraphs 35 and 45 above) is wholly unsubstantiated, even assuming that those provisions applied in the present case.

53. Nor is there any evidence that the applicable domestic legal framework failed to offer adequate and effective safeguards and guarantees against abuse or arbitrariness in relation specifically to events of the type complained of. The applicant company was given ample opportunity to challenge the lawfulness and necessity of the AC's actions and decisions up to the Supreme Court which, contrary to the applicant company's allegations, considered all the principal aspects of the case and gave a duly reasoned decision which was not arbitrary (see paragraphs 17-19 above). Additionally, the Personal Data Protection Act of 2010 guaranteed everyone the right to challenge the processing of his or her personal data in court or with the Parliamentary Commissioner for Human Rights, which had the power to order the authorities to cease processing such data and/or to destroy it, and there is no indication that the available remedies were ineffective in practice, including where the actions or decisions of the State Commissioner of the AC were concerned (see paragraphs 26, 29 and 42 above, and compare *Breyer v. Germany*, no. 50001/12, § 105, 30 January 2020).

54. Secondly, as regards the existence of a legitimate aim and necessity in a democratic society, the Court notes that the AC exercised its power to compel the applicant company, ultimately by imposing a fine on it, to provide telecommunications data for the purpose of investigating a possible breach of competition law. The material presented to the Court demonstrates that there were no serious reasons to doubt that the AC genuinely needed that information in order to verify whether the representatives of two companies bidding in a public procurement procedure had been involved in a cartel, which undoubtedly serves a legitimate aim in protecting the economic well-being of the country (compare, for instance, *DELTA PEKÁRNY a.s. v. the Czech Republic*, no. 97/11, § 81, 2 October 2014).

55. Thirdly, as noted above, the information that the applicant company had in its possession but refused to provide to the AC was limited to the metering data of one telephone number which had been used anonymously. The request was clear and only concerned a period of five months corresponding to the timing of the events being investigated by the AC (see

paragraph 3 above). Even though the data requested could potentially concern a large number of people who were in contact with the telephone number in question, the applicant company was not required to identify them. The AC to which the data had to be disclosed was bound by the rules of confidentiality and was authorised to use them only for the purpose of investigating breaches of competition law (see paragraphs 23 and 26 above). It was not argued that providing the requested data to the AC would have had any repercussions on the applicant company's storage and processing of confidential data relating to its services. Nor could the requirement to disclose the data in question reasonably have resulted in any harm to the applicant company's reputation, since it concerned the authorities' lawful exercise of their statutory powers to access private data for legitimate aims (see, among many other authorities, *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, §§ 234 and 239, 11 January 2022, and *Breyer*, cited above, § 58). In so far as the applicant company may be understood as trying to protect third persons that could potentially be affected, the Court, leaving aside the question about possible domestic remedies available to such third persons, notes that no such claim was made in the domestic proceedings and that, in any event, there is no basis for accepting that the applicant company is entitled to bring an application before the Court on behalf of such unknown third persons.

56. To this it must be added that, even though the amount of the fine imposed on it for refusing to provide the data in question was not negligible (see paragraph 10 above), the applicant company did not argue either in the domestic court or before the Court that the obligation to pay the fine had had serious negative repercussions on its financial situation.

57. The Court finds therefore that the applicant company's present complaints about a breach of its Article 8 rights on account of the events complained of are not supported by persuasive arguments. Therefore, they must be rejected as being manifestly ill-founded in accordance with Article 35 §§ 3 (a) and 4 of the Convention.

II. OTHER ALLEGED VIOLATIONS OF THE CONVENTION

58. In so far as the applicant company also complained of a violation of Article 10 of the Convention and Article 1 of Protocol No. 1 regarding the same facts and legal issues examined by the Court above, those complaints do not disclose any appearance of a violation of the provisions in question. Accordingly, this part of the application is also manifestly ill-founded and must be rejected in accordance with Article 35 §§ 3 (a) and 4 of the Convention.

For these reasons, the Court, unanimously,

Declares the application inadmissible.

Done in English and notified in writing on 8 February 2024.

Victor Soloveytchik Section Registrar	Georges Ravarani President