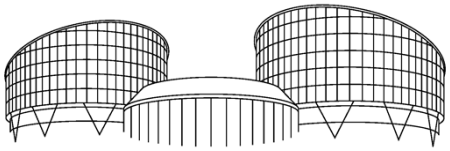

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF GUYVAN v. UKRAINE

(Application no. 46704/16)

JUDGMENT

Art 8 • Positive obligations • Private life • Lack of State protection before a judicial body in relation to the processing of data from the applicant's work mobile telephone by his employer in the context of an internal investigation • Domestic courts' failure to make a full assessment of whether the criteria in respect of the monitoring of the applicant's communications in the workplace were met

Prepared by the Registry. Does not bind the Court.

STRASBOURG

6 November 2025

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 Guyvan v. Ukraine,

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

Kateřina Šimáčková*, President*,
Georgios A. Serghides,
Gilberto Felici,
Andreas Zünd,
Mykola Gnatovskyy,
Vahe Grigoryan,
Sébastien Biancheri*, judges*,
and Victor Soloveytchik, *Section Registrar,*

Having regard to:

the application (no. 46704/16) 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, Mr Petro Dmytrovych Guyvan ("the applicant"), on 26 September 2016;

the decision to give notice to the Ukrainian Government ("the Government") of the complaint concerning an alleged interference with the applicant's right to respect for his private life or his correspondence, within the meaning of Article 8 § 1 of the Convention, and to declare the remainder of the application inadmissible;

the parties' observations;

Having deliberated in private on 14 October 2025,

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

INTRODUCTION

1. The case concerns an alleged violation of the applicant's right to privacy under Article 8 of the Convention, namely the processing of data from his work mobile telephone by his employer in the context of an internal investigation and the employer's refusal to inform him about the data it had thus collected.

THE FACTS

2. The applicant was born in 1958 and lives in Poltava.

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

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

5. The applicant had a mobile telephone which he used both for work and for private calls. According to him, he had used that telephone number as his private number since 2002 and only later had it become his professional mobile telephone number, paid for by his employer, the P. company.

6. On 7 November 2003 the P. company and the mobile phone operator entered into a contract for the provision of mobile services. Among other services, the contract included mobile services for the applicant's telephone.

7. According to Order no. 402 issued by the P. company on 1 November 2005, the telephone number in question was listed as personally assigned to the applicant for work purposes.

8. On 6 May 2010 the P. company issued Order no. 142 on the introduction of limits to the use of mobile services. In accordance with Appendix 1 to that Order, the applicant's use of his work phone for work purposes was subject to a limit of 300 Ukrainian hryvnias (around 30 euros at the material time) per month. Appendix 3 to the Order specified what telephone communications would be considered work-related and therefore paid for by the employer within the established limit. The Order indicated, in particular, that international roaming charges would be paid by the employer only if the person who used the telephone number in question was on an official business trip. Otherwise, the cost of international roaming services and of communications in excess of the limit would be deducted from the employee's salary.

9. In February 2015 an internal investigation was launched into the fact that the applicant's telephone bills indicated that he had used international roaming services on his work phone during periods of time when, according to the staff attendance register, he had been present at his workplace.

10. On 6 and 26 February 2015 the P. company asked the mobile phone operator for detailed information about the relevant calls from the applicant's mobile phone and an indication of the countries in which roaming services had been used by the phone between 1 January 2014 and 31 January 2015. The operator provided the requested information, which contained the following details about the communications: the date and time of the communication, whether the communication had been incoming or outgoing, the foreign telephone company used for roaming services, the country in which the roaming services had been used, the telephone number to or from which the communication with the applicant's mobile phone had been made, whether the communication had been a voice call or a text message, and the duration of the calls.

11. On 11 September 2015 the P. company lodged a criminal complaint against the applicant with the Poltava City Police Department. Those proceedings were pending at the time of the exchange of observations between the parties in the proceedings before the Court. According to the applicant, he learned about the P. company's decision to lodge a criminal complaint against him from the Government's observations, becoming aware of the case for the first time in June 2023.

12. In September 2015 the applicant lodged a claim against the P. company with the Poltava Leninsky District Court. He complained that his employer had been collecting information of a personal nature about him and

had refused his request for access to the data it had thus collected, in violation of the Personal Data Protection Act. At the applicant's request, the court did not consider his claim for damages. Also at the applicant's request, the court joined the mobile phone operator to the proceedings as a third party. The applicant asked the court to declare unlawful the actions of the P. company in collecting and processing his personal data, and to order the defendant to provide him with the information about his personal data which it had received from the mobile phone operator and his colleagues.

13. On 29 October 2015 the applicant was dismissed from his position for being absent from his workplace without a valid reason.

14. On 16 December 2015 the first-instance court found against the applicant. It established that the telephone number used by the applicant had belonged to the P. company and that, as the owner of that telephone number, the P. company had been entitled to seek and obtain detailed information from the mobile phone operator about the services provided. The information about the international roaming services had been requested in order to verify the presence of an employee at his workplace and thus concerned labour relations. The court concluded that there was no indication that the P. company had collected the applicant's personal data, and rejected his claims to the contrary.

15. On 26 January 2016 the Poltava Regional Court of Appeal upheld the decision of the first-instance court. It agreed with the findings of the lower court and took a critical view of the applicant's argument that his use of international roaming services had not been work-related as he had had to reimburse their costs to his employer. The court pointed out that the aim of obtaining the information about the roaming services used by the applicant had been neither to ensure reimbursement of the costs incurred nor to determine where the applicant had been on holiday or with whom he had been communicating; rather, the aim had been to establish whether or not he had been present at his workplace during working hours.

16. On 14 April 2016 the Supreme Court upheld the decisions of the lower courts, confirming that the information about the international roaming services used by the applicant's work phone did not constitute his personal data.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. CONSTITUTION

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

Article 32

"No one shall be subject to interference in his or her personal and family life, except in cases envisaged by the Constitution of Ukraine.

The collection, storage, use and dissemination of confidential information about a person without his or her consent shall not be permitted, except in cases determined by law, and only in the interests of national security, economic welfare and human rights ...”

Article 34

“... 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 disclosure of information received confidentially, or supporting the authority and impartiality of justice.”

II. PERSONAL DATA PROTECTION ACT OF 2010

18. The collection and use of personal data is further regulated by the Personal Data Protection Act of 2010. Under section 2 of the Act, “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. 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. Referred to by the domestic courts in the present case, section 7(2)(2) of the Act concerns one of the exceptions to the prohibition on the processing of personal data, namely if the processing “is necessary for the performance of the duties of a [data] controller in the sphere of labour relations in accordance with the law, provided that an adequate level of protection is ensured”. Under section 22 of the Act, the Parliamentary Commissioner for Human Rights and the courts are responsible for ensuring that legislation on personal data protection is observed.

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

19. 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.

20. 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.

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

21. 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 ..."

Article 8 – Additional safeguards for the data subject

"Any person shall be enabled ...

(d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

22. The applicant complained that the courts failed to protect his right to privacy contrary to Article 8 of the Convention in relation to his employer having processed his personal data. That Article reads as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. Admissibility

23. The Government submitted that the applicant had not exhausted domestic remedies as he had not challenged the actions of the mobile phone operator. They further maintained that the applicant's complaint was groundless as the information collected by his employer had not been confidential and the information obtained about his calls – which had not entailed accessing their content – had been purely technical. They submitted that the employer's collection of that information had not interfered with the applicant's right to respect for his private life.

24. The applicant disagreed.

25. In so far as the Government pleaded non-exhaustion of domestic remedies, the Court notes that, in his application to the Court, the applicant complained of the domestic courts' failure to protect him against his employer's unlawful collection of his personal data, submitting that he had raised that complaint before the domestic courts and that they had concluded that the information collected did not constitute personal data. There is no explanation in the Government's objections as to the extent to which the involvement of the mobile phone operator as a defendant or a co-defendant rather than a third party could have affected the conclusions of the domestic courts. The Court considers that the applicant took sufficient steps at the national level to bring the domestic authorities' attention to issue at stake. It therefore dismisses this objection.

26. As to the Government's second objection – namely, that the present application is groundless – the Court considers that, in the circumstances of the present case, addressing that objection will require it to look into the merits of the applicant's complaint under Article 8 of the Convention. For this particular reason, it will examine the second objection when dealing with the merits (see, *mutatis mutandis*, *Denisov v. Ukraine* [GC], no. 76639/11, § 93, 25 September 2018).

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

B. Merits

1. The parties' submissions

28. The applicant maintained that a violation of his right to privacy under Article 8 of the Convention had taken place, namely the processing of data from his work mobile telephone by his employer in the context of an internal investigation and his employer's refusal to inform him about the data it had collected. From the relevant arrangements on the use of work telephone numbers, it was clear that the telephone could be used for non-work-related communications, especially when communicating from abroad. The applicant had asked the domestic authorities to protect him from the unlawful collection and processing of his personal data, but the courts at three levels of jurisdiction had rejected his complaints on the grounds that personal data-protection guarantees were not applicable in the context of labour relations between an employee and his or her employer.

29. The Government maintained that the present case concerned a dispute between two private parties – the applicant and his employer – which implied that the State was not directly involved but had certain positive obligations to ensure respect for the rights protected by Article 8. They referred to the relevant factors concerning the monitoring of communications in the workplace listed in *Bărbulescu v. Romania* ([GC], no. 61496/08, §§ 121-22, 5 September 2017), namely prior notification to employees about the possible monitoring of their communications, the extent and intrusiveness of the monitoring, its justification, the existence of less intrusive alternatives, the consequences for employees, and the provision of adequate safeguards. The Government maintained that the authorities had taken all those factors into consideration. According to the Government, the P. company had collected purely technical information in a manner which had been foreseeable in view of its orders concerning the use of work telephones, and the collection of information in such a way could not constitute interference with the applicant's right to respect for his private life. They further submitted that the domestic courts had found that, as regards the applicant's personal communications, the P. company had not collected his personal data and the data that had been collected had not been confidential. They stressed that the employer had not had and could not have had access to the actual content of the applicant's communications.

2. The Court's assessment

(a) Applicability of Article 8

30. The Court reiterates that the notion of "private life" is a broad and evolving concept, which goes beyond an individual's private sphere and encompasses to a certain extent his or her interactions in public and professional settings as well (see *López Ribalda and Others v. Spain* [GC], nos. 1874/13 and 8567/13, §§ 87-91, 17 October 2019, with further references). The notion of "private life" includes, among many other things, information about the person's location at a given moment in time (see, *mutatis mutandis*, *Uzun v. Germany*, no. 35623/05, §§ 51-52, ECHR 2010 (extracts), and *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, no. 26968/16, §§ 95-96, 13 December 2022).

31. In the present case, the information sought and obtained by the applicant's employer from the mobile phone operator related to the use of roaming services by the mobile phone that had been individually assigned to the applicant for work purposes. From the arrangements indicated in the Order of 6 May 2010 (see paragraph 8 above), it appears that the applicant was permitted to use the work telephone number assigned to him for making private calls, including from abroad, on condition that he reimbursed the cost of those calls. Indeed, the P. company was able to obtain information from the mobile phone operator and to collect and process that information for specific purposes. However, that did not deprive the data of its personal character, such as the location of the applicant in a particular country on a particular date. Such information, as well as information about the recipients of his communications, could be characterised as his personal data.

32. The Court considers that Article 8 is applicable in the present case.

(b) Compliance with the requirements of Article 8

(i) General principles

33. The Court observes that, in the present case, the measure complained of by the applicant was imposed by his employer, a private company, and cannot therefore be analysed as an "interference" by a State authority with the exercise of his Convention rights. The applicant nevertheless took the view that, by refusing to examine his complaint that the use of his personal data had been unlawful, the domestic courts had not provided effective protection of his right to respect for his private life.

34. The Court reiterates that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in effective respect for private or family life. These obligations may necessitate the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals

between themselves. The responsibility of the State may thus be engaged if the facts complained of stemmed from a failure on its part to secure to those concerned the enjoyment of a right enshrined in Article 8 of the Convention (see *López Ribalda and Others*, cited above, § 110, with further references).

35. While the boundaries between the State's positive and negative obligations under the Convention do not lend themselves to precise definition, the applicable principles are nonetheless similar. In both contexts regard must be had in particular to the fair balance that has to be struck between the competing private and public interests, subject in any event to the margin of appreciation enjoyed by the State. The margin of appreciation goes hand in hand with European supervision, embracing both the legislation and the decisions applying it, even those given by independent courts. In exercising its supervisory function, the Court does not have to take the place of the national courts but to review, in the light of the case as a whole, whether their decisions were compatible with the provisions of the Convention relied upon (ibid., § 111, with further references).

36. The Court further reiterates that the choice of the means calculated to secure compliance with Article 8 of the Convention in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting States' margin of appreciation. There are different ways of ensuring respect for private life, and the nature of the State's obligation will depend on the particular aspect of private life that is at issue. In certain circumstances, the fulfilment of positive obligations imposed by Article 8 requires the State to adopt a legislative framework to protect the right at issue. Concerning the gravest acts, this obligation may go as far as requiring the adoption of criminal-law provisions. In respect of less serious acts between individuals which may affect the rights protected under Article 8, the Court takes the view that Article 8 leaves it to the discretion of States to decide whether or not to pass specific legislation, and it verifies that the existing remedies were capable of providing sufficient protection of the rights at issue (ibid., §§ 112-13).

37. In *Bărbulescu* (cited above, § 121), the Court defined the criteria to be taken into consideration in respect of the monitoring of communications in the workplace, namely whether the employee has been notified of the possibility that the employer might take measures to monitor communications and of the implementation of such measures, the extent of such monitoring and the degree of its intrusion into the employee's privacy, whether the employer has provided legitimate reasons to justify monitoring, whether it would have been possible to implement less intrusive methods and measures, the consequences of the monitoring for the employee subjected to it, and whether the employee has been provided with adequate safeguards against arbitrariness. The Court further held that "the domestic authorities should ensure that an employee whose communications have been monitored has access to a remedy before a judicial body with jurisdiction to determine, at

least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful" (ibid., § 122).

38. In the Court's opinion, it is for the domestic courts to conduct a proportionality analysis of the competing rights and to give due consideration to data protection issues. Failure to address the Convention issue at stake, be it on account of the state of the domestic legislation or because of its interpretation by the national authorities, will fall foul of the requirements of Article 8 (see *Liebscher v. Austria*, no. 5434/17, §§ 64-69, 6 April 2021).

(ii) Application of these principles in the present case

39. Turning to the present case, the Court notes that, from the arrangements indicated in the P. company's Order of 6 May 2010 (see paragraph 8 above) and the relevant contract with the mobile phone operator (see paragraph 6 above), it appears that the P. company was entitled to receive information from the mobile phone operator for the purpose of establishing what calls and messages fell within the category of work communications and, accordingly, whether their costs should be borne by the company or the applicant. However, the employer's requests of 6 and 26 February 2015 (see paragraph 10 above) were made with the very different and unrelated purpose of collecting and processing data which could reveal the applicant's location abroad on particular dates. Furthermore, the data in question included information about the telephone numbers with which the applicant had been in contact and the countries in which roaming services had been provided, even though, by the authorities' own admission, that information was not necessary for the purpose of establishing whether or not the applicant had been at his workplace (see paragraph 15 above). The Court considers that the collection and processing of data in such a way affected the applicant's privacy. Whether such collection and processing was justified in the light of the *Bărbulescu* criteria was primarily a question for the domestic authorities to answer. However, the national judicial bodies did not make a full assessment of that issue as they instead concluded that the information obtained by the P. company from the mobile phone operator had not concerned the applicant's personal data.

40. The foregoing considerations are sufficient to enable the Court to conclude that the applicant was denied State protection before a judicial body that would have determined whether the criteria in respect of the monitoring of his communications in the workplace had been met (see paragraphs 37 and 38 above). It follows that the State failed to fulfil its positive obligations under Article 8 of the Convention.

41. There has accordingly been a violation of that Article.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

42. The applicant did not submit a claim for just satisfaction. Accordingly, the Court considers that there is no call to award him any sum on that account.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 8 of the Convention.

Done in English, and notified in writing on 6 November 2025, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Victor Soloveytchik Registrar	Kateřina Šimáčková President