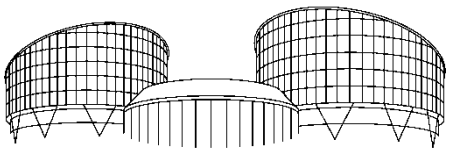
dirittifondamentali.it

La CEDU sulla violazione dell'art. 8 della Convenzione.
(CEDU, sez. V, sent. 13 febbraio 2025, ric. n. 51409/19)

La questione sottoposta all'attenzione della Corte riguarda la presunta violazione dell'art. 8 della Convenzione. Nel caso di specie, la ricorrente lamentava la lesione del proprio diritto alla riservatezza nella corrispondenza, posto che la condanna inflittale dai giudici interni per evasione fiscale si basava su e-mail ottenute dalla polizia tramite un'ordinanza emessa ai sensi dell'articolo 88a del Codice di procedura penale. In particolare ella contestava la legittimità di tale prova, ritenendo assente una base giuridica adeguata, poiché l'articolo 88a permetteva di ottenere solo dati sul traffico delle comunicazioni, non il loro contenuto.
La Corte riconosce l'ingerenza delle autorità nella sfera di riservatezza della ricorrente, ma ritiene di dover valutare, ai fini della violazione, se questa sia giustificata ai sensi dell'art. 8 § 2 della Convenzione. Tuttavia, già nell'esaminare il criterio della conformità alla legge, rileva che i quattro gradi di tribunali nazionali nel pronunciarsi hanno fatto riferimento a tre diverse disposizioni (artt. 88, 88a e 158d del c.p.p.), dimostrando incoerenza e mancanza di chiarezza nel procedimento interpretativo. Inoltre, nessun giudice ha affrontato adeguatamente le lamentele della ricorrente sul dovere di riservatezza del fornitore e sul divieto di archiviazione del contenuto delle comunicazioni. La Corte osserva inoltre che la versione dell'art. 88a, su cui si sono basate Corte Suprema e Corte Costituzionale, non era in vigore al momento dell'ordinanza. Pertanto, conclude che l'ingerenza non era conforme alla legge e accerta la violazione dell'art. 8 della Convenzione.
Diversamente, i giudici hanno ritenuto non fondata la questione relativa alla violazione dell'art. 6 CEDU, dal momento in cui, nonostante le prove siano state ottenute in contrasto con l'art. 8, il loro utilizzo non ha automaticamente determinato una violazione del diritto a un equo processo.

***



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

FIFTH SECTION

CASE OF XXX v. THE CZECH REPUBLIC

(Application no. 51409/19)

JUDGMENT
STRASBOURG

13 February 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 XXX v. the Czech Republic,

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

Mattias Guyomar, *President*,
María Elósegui,
Armen Harutyunyan,
Stéphanie Mourou-Vikström,
Diana Sârcu,
Kateřina Šimáčková,
Mykola Gnatovskyy, *judges*,
and Victor Soloveytchik, *Section Registrar*,

Having regard to:

the application (no. 51409/19) against the Czech Republic lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Czech national, Ms Omissis ("the applicant"), on 24 September 2019;

the decision to give notice to the Czech Government ("the Government") of the complaints concerning Articles 6 § 1 and 8 of the Convention;

the parties' observations;

Having deliberated in private on 21 January 2025,

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

INTRODUCTION

1. The application concerns the applicant's criminal conviction based mainly on the content of her email communications with another convict, which the police had obtained following a judicial order issued pursuant to a provision relating to data on telecommunications traffic, which, according to the applicant, provided no legal basis for the interference in question (Articles 6 § 1 and 8 of the Convention).

THE FACTS

2. The applicant was born in Omissis and lives in Omissis. She was represented by Omissis, a lawyer practising in Brno.

3. The Government were represented by their Agent, Mr P. Konůpka, of the Ministry of Justice.

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

5. On 14 November 2011 a judge of the Prague 3 District Court issued an order under Article 88a of the Code of Criminal Procedure (hereinafter "CCP") enjoining a communications service provider to provide the police with all data on past telecommunications traffic passing through the mailbox of the Omissis company from the earliest possible date until 14 November 2011, including all available information about the registered user of that mailbox (registration data, IP addresses) and the contents of all messages contained therein. The order was issued at the request of a prosecutor, upon a proposal by the police, in a case of suspected tax evasion by Omissis, as the authorised representative of the Omissis company, together with the representatives of roughly 40 other companies, some of whom remained unidentified. The order mentioned that the Constitutional Court's judgment no. Pl. ÚS 24/10 (see paragraph 24 below) repealing section 97(3) of the Electronic Communications Act (Law no. 127/2005) was not an obstacle since all the requisite guarantees were met in the present case; namely, the order was aimed at obtaining information necessary to identify the perpetrators of an offence and to document their criminal activities, which were serious and punishable by a prison sentence ranging from five to ten years.

6. On 30 November 2011, the communications service provider provided the police with the available registration data and the contents of the mailbox, including messages written by the applicant which had been forwarded to Omissis by another suspect. The service provider observed that, in accordance with the Constitutional Court's judgment no. Pl. ÚS 24/10, it did not store operational and location data, which could thus not be provided.

7. After inspecting the applicant's messages, the police opened a criminal investigation into her activities.

8. On 16 August 2012 the applicant was charged with tax evasion for entering invoices for fictitious leases of advertising space in accounting records and filing a tax return based on those invoices. After the charges had been brought against her, the applicant unsuccessfully sought to have her email messages removed from the case file, arguing that the content of those messages could not be considered communications data within the meaning of Article 88a of the CCP. She further argued that communications service providers were not authorised to store the content of any messages; thus, the communications service provider should have refused to forward the content of her communications to the police.

9. On 24 June 2013 the applicant was indicted as an accomplice to tax evasion.

10. On 18 March 2015 the Prague Municipal Court (hereinafter also "the first-instance court") found the applicant guilty as charged and sentenced her to two years' imprisonment, suspended, and to the payment of a financial penalty of 50,000 Czech crowns (approximately 2,000 euros). According to the court, the applicant's emails that had been forwarded to Omissis proved, in the light of their content and of the order of events, that the leasing agreements and the corresponding invoices had been backdated. The advertising could not have taken place as alleged by the defendants and as falsely stated in the documents.

As to the lawfulness of the contested evidence (email communications), the court held that the relevant order should have been based on Article 88 of the CCP, which related to the content of communications (as opposed to Article 88a, which related to communications data). Nevertheless, this was considered merely a formal shortcoming, given that the order had been issued by a competent court and that all the conditions laid down in Article 88 had been met (criminal proceedings had been initiated against Omissis for a particularly serious offence that was punishable by five to ten years' imprisonment and there were reasonable grounds to believe that the issuance of the order would lead to the disclosure of facts relevant to those criminal proceedings).

11. On 23 September 2016 the Prague High Court (hereinafter also "the appellate court") dismissed an appeal by the applicant in which she argued that the evidence in question could not have been obtained under Article 88 of the CCP as held by the first-instance court, since that provision related solely to the interception and recording of future communications, the formal requirements for which had not been met. The High Court emphasised that, indeed, the main difference between Article 88 and Article 88a was that the former regulated the interception and recording of future communications, while the latter related to data on past telecommunications traffic. Therefore, the judge of the Prague 3 District Court had correctly relied on Article 88a of the CCP for the purpose of obtaining email communications made prior to the order. Lastly, the High Court noted that the order had been issued by a court of competent jurisdiction and had been duly reasoned.

12. On 28 March 2018 the Supreme Court dismissed as manifestly ill-founded an appeal on points of law lodged by the applicant in which she argued that her email communications should not have been admitted as evidence because they had been unlawfully obtained under Article 88a of the CCP and that the content of those messages had been obtained unlawfully from the communications service provider. The Supreme Court held that the content of email communications could not have been obtained through the procedure provided for in Article 88, as an order based on that provision could only concern future – and not past – communications. Furthermore, a court order issued under Article 88a could only be used to obtain communications data, that is, operational and location data within the meaning of the Electronic Communications Act. The same followed from the decision of the Constitutional Court no. III. ÚS 3812/2012 of 3 October 2013, according to which data stored on tracked computers should be obtained under Article 158d of the CCP, relating to the surveillance of persons and objects. The Supreme Court further pointed out that, in accordance with Article 158b, the surveillance of persons and objects under Article 158d could be authorised in criminal proceedings for an intentional offence only where the aim pursued could not be achieved in any other way or would otherwise be considerably more difficult to achieve. Such surveillance was subject to prior authorisation by a judge if it was to interfere with the privacy of correspondence. However, Article 158d did not lay down any requirements as to the reasoning of orders issued under that provision, nor did it offer any guarantees as to the proportionality between the interference with privacy and the seriousness of the offence in question. On the other hand, Article 88a laid down conditions for issuing a court order and specified the range of offences for which it could be issued. It followed that the latter provision, which also ensured the proportionality between the interference with privacy and the seriousness of the offence in question, was a specific case of surveillance of persons within the meaning of Article 158d. The Supreme Court thus concluded that, since Article 88a imposed

stricter requirements for the issuance of a court order than did Article 158d, and given the inconsistent practices at the time when the order challenged by the applicant had been issued, the evidence obtained through the procedure provided for in Article 88a could not be considered inadmissible.

13. In its decision no. III. ÚS 2374/18 of 27 March 2019, the Constitutional Court dismissed as manifestly ill-founded a constitutional appeal by the applicant in which she complained that the guilty verdict had been based solely on the content of her email correspondence, which had been provided to the police on an inappropriate legal basis. Referring to the Supreme Court's decision, the Constitutional Court stated that, at the time when the order in question had been issued (that is, two years prior to its decision no. III. ÚS 3812/12), court practice had been inconsistent and both Articles 88a and 158d had been used to obtain the content of email communications. However, as the Supreme Court had rightly pointed out, while Article 158d did not offer any specific guarantees regarding the proportionality between the interference and the seriousness of the offence, Article 88a provided stricter conditions in this regard. Therefore, obtaining the content of email communications under Article 88a could not entail constitutionally unacceptable consequences.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. THE CODE OF CRIMINAL PROCEDURE AS IN FORCE AT THE RELEVANT TIME

14. Under Article 88 §§ 1 and 2, in the context of criminal proceedings for a particularly serious crime, the interception and recording of telecommunications traffic (*odposlech a záznam telekomunikačního provozu*) could be ordered if it could be reasonably assumed that it would disclose facts relevant to the criminal proceedings. Such an order was to be issued by the judge presiding the trial or, at the pre-trial stage, by a judge acting upon a proposal by a prosecutor.

15. Pursuant to Article 88a § 1, if data on past telecommunications traffic *(údaje o uskutečněném telekomunikačním provozu)* which were subject to telecommunications privacy or fell under the protection of personal data were necessary in order to clarify circumstances relevant to criminal proceedings, the presiding judge, or a judge at the pre-trial stage, would order persons or entities providing telecommunications services to disclose such data. The order had to be issued in writing and had to be reasoned.

16. In its amended version in force since 1 October 2012, Article 88a § 1 provided that, if it was necessary, for the purposes of criminal proceedings concerning an intentional offence punishable by up to three years' imprisonment, to disclose data on telecommunications traffic which were subject to telecommunications privacy or which fell under the protection of personal data, and if the aim pursued could not be achieved in any other way or would otherwise be considerably more difficult to achieve, the presiding judge or, at the pre-trial stage, a judge acting upon a proposal by a prosecutor, would order the disclosure of such data. Such an order had to be issued in writing and had to be reasoned.

17. Under Article 158b §§ 1 and 2, the police were entitled, in the context of any criminal proceedings for an intentional offence, to use operative investigative means (*operativně pátrací prostředky*), including the surveillance of persons and objects (*sledování osob a věcí*). Operative

investigative means could be used only if the aim sought could not be achieved in any other way or would otherwise be considerably more difficult to achieve.

18. Under Article 158d §§ 1, 3, 4, the surveillance of persons and objects consisted in the covert collection of information on persons and objects by technical or other means. If it was to interfere with the privacy of correspondence, surveillance was subject to prior authorisation by a judge. Such authorisation could be issued solely upon written request and had to specify the period over which the surveillance was to be conducted, which could not exceed six months.

II. LAW NO. 127/2005 ("ELECTRONIC COMMUNICATIONS ACT") AS IN FORCE UNTIL 11 APRIL 2011

19. Under section 90(1), operational data (*provozní údaje*) were any data processed for the purpose of transmitting a message through an electronic communications network or for billing purposes.

20. Under section 91(1), location data (*lokalizační údaje*) were any data processed in an electronic communications network which identified the geographical location of the terminal equipment of a user of a publicly available electronic communications service.

21. Pursuant to section 97(3), legal or natural persons providing a public communications network or a publicly available electronic communications service were obliged to store operational and location data generated or processed in the course of their activities for a period ranging from six to twelve months (after which such data had to be deleted), and, upon request, to provide them to the authorities authorised to request them; at the same time, the communications service providers were to ensure that the content of the communications was not stored.

III. RELEVANT DOMESTIC CASE-LAW

A. Case-law concerning the Code of Criminal Procedure

22. In its judgment no. Pl. ÚS 24/11 of 20 November 2011, the Plenary of the Constitutional Court declared Article 88a of the CCP unconstitutional, with effect from 1 October 2013, holding that the conditions for access to data on telecommunications traffic laid down by that provision were overly general, vague and therefore insufficient. The Constitutional Court emphasised, *inter alia*, that the contested provision had not offered any guarantees as to the proportionality between the interference with privacy and the seriousness of the offence.

23. In its decision no. III. ÚS 3812/12 of 3 October 2013, the Constitutional Court stated that the data stored on tracked computers (that is, not the data on telecommunications traffic) could be obtained on the basis of a court order issued under Article 158d of the CCP relating to the surveillance of persons and objects.

B. Case-law concerning the Electronic Communications Act

24. In its judgment no. Pl. ÚS 24/10 of 22 March 2011, the Plenary of the Constitutional Court declared section 97(3) and (4) of the Electronic Communications Act unconstitutional and repealed it as of the date of publication of that judgment in the Collection of Laws (11 April 2011). It stated, in particular, that the general and preventive collection and retention of operational and location data amounted to significant interference with the right to privacy and should be limited to exceptional situations where the legitimate aim pursued could not be achieved by other means,

provided that specific, detailed and effective safeguards against arbitrariness were in place, which the impugned provision did not offer at the material time.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

25. The applicant complained that her email communications had been obtained without a proper legal basis, in breach of the guarantees of Article 8 of the Convention, which 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

26. The Court notes that this complaint 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

27. As she had done before the domestic courts, the applicant focused her Article 8 complaint on the purported unlawfulness of the interference. She argued that, in order to obtain the content of her email messages, the domestic authorities had relied on Article 88a of the CCP, which only allowed communications data to be obtained, not the content of communications. While it was true that the Constitutional Court had later ruled that the content of communications could be obtained under Article 158d of the CCP (see paragraph 23 above), that procedure, which moreover lacked sufficient guarantees, concerned a different situation, namely, data stored on a tracked computer belonging to a person subject to surveillance. Moreover, it was not possible under any of those provisions, and in a situation where section 97(3) of the Electronic Communications Act had been repealed, to order the communications service provider to make the content of private communications available to the police, which was what had happened here. Thus, in the applicant's view, the impugned order had relied on an inappropriate legal basis.

28. The Government acknowledged that there had been an interference with the applicant's rights under Article 8 but considered it to have been lawful since both Articles 88a and 158d of the CCP pursued the same objectives and were used in practice to obtain the content of email communications. The applicant could therefore have foreseen that her right to privacy of correspondence might be interfered with in this way. The Government maintained that Article 88a of the CCP, on which the order had been based in the present case, offered more guarantees than Article 158d of the CCP; the applicant's rights had thus enjoyed greater protection. While they conceded that the relevant practice had not been normalised until the decision of the Constitutional Court of 3 October 2013, the Government pointed out that it was natural that

domestic case-law would evolve in response to the development of new technological means of communication.

29. They also emphasised that, in the present case, the interference had been proportionate to the nature of the criminal offence in question, the impugned order had been confined to a period that corresponded to the time when the offence had allegedly been committed and information had been gathered only to extent necessary for the investigation. Lastly, the Government observed that four levels of domestic courts had considered the applicant's arguments, finding the impugned order lawful and giving sufficient reasons for their decisions.

2. *The Court's assessment*

(a) General principles

30. The Court notes at the outset that Article 8 of the Convention protects the confidentiality of all the exchanges in which individuals may engage for the purposes of communication, whatever the content of the correspondence concerned and whatever form it may take (*Michaud v. France*, no. 12323/11, § 90, 6 December 2012, ECHR 2012; *Dragoş Ioan Rusu v. Romania*, no. 22767/08, § 33, 31 October 2017). Email communications, including those of a professional nature, fall under the concept of correspondence (*Copland v. the United Kingdom*, no. 62617/00, § 41, 7 December 2006, ECHR 2007; and *Tena Arregui v. Spain*, no. 42541/18, § 31, 11 January 2024).

31. The Court reiterates that any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim (*Roman Zakharov v. Russia* [GC], no. 47143/06, § 227, 4 December 2015).

32. The Court has consistently held that when it comes to the interception of communications for the purpose of a police investigation, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. In particular, in order to comply with the requirement of the "quality of the law", a law which confers discretion must indicate the scope of that discretion, although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law. The degree of precision required of the "law" in this connection will depend upon the particular subject-matter. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive – or to a judge – to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Amann v. Switzerland* [GC], no. 27798/95, § 56, ECHR 2000-II; and *Bykov v. Russia* [GC], no. 4378/02, § 78, 10 March 2009).

33. The Court has already recognised the impossibility of attaining absolute certainty in the framing of laws and the risk that the search for certainty may entail excessive rigidity. Many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose

interpretation and application are questions of practice (see *Klaus Müller v. Germany*, no. 24173/18, § 50, 19 November 2020). The Court's role is to assess the relevant domestic law in force at the time in relation to the requirements of the fundamental principle of the rule of law. Such a review inevitably entails some degree of abstraction. Nevertheless, in cases arising from individual applications, the Court must as a rule focus its attention not on the law as such but on the manner in which it was applied to the applicant in the particular circumstances (see *Goranova-Karaeneva v. Bulgaria*, no. 12739/05, § 48, 8 March 2011, and *Dragojević v. Croatia*, no. 68955/11, § 86, 15 January 2015).

(b) Application of these principles to the circumstances of the present case

(i) Whether there was an interference

34. There is no dispute between the parties that obtaining the content of the applicant's email communications contained in Omissis's mailbox, content which was used as evidence in the criminal proceedings against the applicant, interfered with her right to respect for her private life and correspondence. In this regard, the Court observes that the measure was applied to the email account of a third person to whom the applicant's messages had been forwarded by another person. With regard to the fact that those email communications were of a professional nature and that the extent of the information thereby disclosed about the applicant was limited, such a measure can be considered less likely to interfere with her rights under Article 8 than would a measure to obtain the contents of her own private mailbox or even the interception of some of her telephone conversations on a third party's line. Nevertheless, it can hardly be argued that by sending her emails the applicant automatically waived her right to privacy simply because there was a hypothetical possibility that those emails could be forwarded to others or obtained by the authorities. Rather, she had a reasonable expectation that the privacy of her communications would be respected and protected (see *Bărbulescu v. Romania* [GC], no. 61496/08, § 73, ECHR 2017; and *Benedik v. Slovenia*, no. 62357/14, § 101, 24 April 2018).

35. Thus, having regard to the principles established in its case-law, the Court finds that the implementation of the court order for the transfer of the content of all messages contained in Omissis's mailbox, which resulted in the applicant's email messages being made available to the police and, subsequently, in the evidence thus collected being used to initiate criminal proceedings against her, amounted to an interference with the applicant's right to respect for her private life and correspondence as protected by Article 8 § 1.

(ii) Whether the interference was justified

36. The Court reiterates that it is primarily for the national authorities, notably the courts, to interpret and apply domestic law. However, the Court is required to verify whether the way in which this is done produces consequences that are consistent with the principles of the Convention as interpreted in the light of the Court's case-law (see *Benedik*, cited above, § 123). In particular, the Court has previously emphasised the importance of sufficient safeguards against arbitrariness and abuse when it comes to the interception, retention and access by the authorities of both the content of communications and the related communications data (see *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 395, 11 January 2022, and *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, §§ 248-49, 277, 25 May 2021).

37. In the present case, it is the content of the applicant's email correspondence that was obtained pursuant to an order issued by a judge of the Prague 3 District Court under Article 88a of the CCP relating to communications data. Throughout the criminal proceedings and before the Court, the applicant contended that this material had been obtained unlawfully because, under the relevant domestic legislation, communications data did not include the content of the messages exchanged and, moreover, communications service providers were not authorised to store and disclose the content of such messages (see paragraph 8 *in fine* above). Hence, according to the applicant, Article 88a of the CCP did not provide a legal basis for securing the email messages in question.

38. The Court notes that, at the material time, Article 88a of the CCP (see paragraph 15 above) provided that a judge could order telecommunications providers to disclose communications data – which that provision defined as data on past telecommunications traffic, falling under the privacy of telecommunications or the protection of personal data – if such data were necessary in order to clarify circumstances relevant to criminal proceedings. In the present case, the Supreme Court itself stated (see paragraph 12 above) that the above provision referred to operational and location data under the Electronic Communications Act (see paragraphs 19-20 above). In addition, as submitted by the applicant, section 97(3) of the Electronic Communications Act, which had been in force until 11 April 2011 (prior to the issuance of the order in the present case), provided, *inter alia*, that communications service providers, when storing communications (operational and location) data, were to ensure that the content of the communications had not been stored. The Constitutional Court repealed this provision in its judgment no. Pl. ÚS 24/10 of 22 March 2011 (see paragraph 24 above), albeit for reasons that did not relate to that particular issue, such that the subsequent amendment of the same provision by Law no. 273/2012, which came into force on 1 October 2012, provided for the same obligation not to store the content of communications.

39. It can be surmised from the above considerations that the court order in question was issued after the above-mentioned judgment of the Constitutional Court of 22 March 2011 striking down section 97(3) of the Electronic Communications Act and before the entry into force of the subsequent amendment of that provision, namely, during a limited period where there was no provision barring communications service providers from storing the content of communications. However, neither the domestic courts nor the Government addressed the applicant's argument that the content of the messages should not have been stored; in particular, they did not refer to any legal provision in force at the material time on the basis of which communications service providers might store and transmit the content of communications or the police might access an individual's mailbox. Yet, when the Prague 3 District Court had ordered the communications service provider, on the basis of Article 88a of the CCP, to make available the content of all emails in Omissis's mailbox to the police, the provider had complied with that order (see paragraph 6 above).

40. As to the applicant's complaints concerning the inappropriate legal basis on which the content of her email correspondence were obtained, the Court observes that they were examined, in the criminal proceedings against her, by four levels of domestic courts. However, three of those courts reached a different conclusion as to which legal provision could serve as a legal basis for obtaining this material.

41. Indeed, the first-instance court held that the order should have been based on Article 88 of the CCP (not Article 88a), which regulated the interception of telephone communications.

Nevertheless, since all the conditions laid down in Article 88 of the CCP were met in the present case, it concluded that the evidence had been lawfully obtained and was admissible. By contrast, the appellate court took the view that Article 88 of the CCP only regulated the interception and recording of *future* exchanges and therefore that the evidence had been lawfully obtained under Article 88a of the CCP. Subsequently, the Supreme Court endorsed the applicant's argument that the content of the messages stored in a mailbox could not be obtained under Article 88a of the CCP, as this provision referred only to communications data. At the same time, it held that it was possible to obtain such evidence under Article 158d of the CCP, which related to the surveillance of persons and objects, as also followed from the Constitutional Court's decision no. III. ÚS 3812/12 of 3 October 2013. Acknowledging that, prior to that decision, court practice had been inconsistent, the Supreme Court compared the two provisions (Articles 88a and 158d of the CCP) and pointed out that, unlike Article 88a, Article 158d did not lay down any specific requirements as to the reasoning of the orders issued thereunder, nor did it offer any guarantees as to the proportionality between the interference with privacy and the seriousness of the offence in question. Given that Article 88a placed even stricter requirements on interference, the Supreme Court concluded that the evidence in issue in the present case could not be considered to have been obtained unlawfully, even if it had been so on the basis of Article 88a and not on the basis of Article 158d. Ultimately, the Constitutional Court endorsed the findings of the Supreme Court.

42. The Court has previously held that in any system of law, including criminal law, there is an inevitable element of judicial interpretation. The Convention cannot be read as outlawing the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen. The Court has already held that these principles apply also in the context of interferences with private life in criminal proceedings (see *Uzun v. Germany*, no. 35623/05, § 62, ECHR 2010 (extracts)). The Court observes, however, that in the case at hand the domestic courts referred in total to three provisions (Articles 88, 88a and 158d of the CCP) as potentially serving as a legal basis for the interference with the confidentiality of the applicant's email communications. More importantly, both the Supreme Court and the Constitutional Court endorsed the applicant's argument to the effect that Article 88a of the CCP, under which the impugned order had been issued, did not apply to the content of email communications. Furthermore, in finding that Article 88a of the CCP imposed stricter requirements and offered more guarantees than Article 158d of the CCP, in particular because it specified the range of offences in respect of which it could be used, those courts referred to a later version of that provision (see paragraph 16 above), as amended following the Constitutional Court's judgment no. Pl. ÚS 24/11 of 20 November 2011, which had declared the (relevant) previous version of Article 88a of the CCP unconstitutional (see paragraph 22 above). In other words, the version of Article 88a of the CCP which both the Supreme Court and the Constitutional Court took into consideration to conclude that the content of the applicant's messages had been obtained lawfully was not yet in force at the time when the order in question had been issued. Therefore the Government's argument based on their findings that Article 88a of the CCP offered more guarantees than Article 158d of the CCP cannot stand.

43. In sum, the Court notes that, firstly, the Prague 3 District Court ordered the communications service provider to make available to the police the contents of Omissis's mailbox, including the applicant's email communications, even though it is apparent that domestic law did not allow

providers to store the content of such communications. Moreover, the courts did not adequately address the applicant's specific complaints raised in this respect with regard to the provider's duty of confidentiality (see, *mutatis mutandis*, *Azer Ahmadov v. Azerbaijan*, no. 3409/10, § 73, 27 July 2021). Nor did the Government rebut the applicant's arguments in support of these complaints. Secondly, the way in which the domestic courts interpreted and applied the relevant legal provisions was incoherent and demonstrated the lack of clarity of the legal framework in question (see, *mutatis mutandis*, *Lia v. Malta*, no. 8709/20, § 67, 5 May 2022).

44. For the above reasons, the Court cannot but conclude that the interpretation and application of domestic law in the applicant's case lacked clarity and consistency and, therefore, were not foreseeable for the purposes of Article 8 of the Convention. The interference with the applicant's rights under Article 8 was therefore not "in accordance with the law".

45. In the light of this conclusion, the Court considers that it is not necessary to examine whether the interference in the present case pursued one or more legitimate aims or was necessary in a democratic society for the purposes of Article 8 § 2.

46. Accordingly, the Court concludes that there has been a violation of Article 8 in this case.

II. ALLEGED VIOLATION OF ARTICLE 6 § 1 OF THE CONVENTION

47. The applicant complained that her criminal conviction was based mainly on the evidence obtained in breach of Article 8 of the Convention. She relied on Article 6 § 1 of the Convention, which, in so far as relevant, reads as follows:

"In the determination of ... any criminal charge against him, everyone is entitled to a fair ... hearing ... by [a] ... tribunal ..."

A. Admissibility

48. The Court notes that this complaint is linked to the one examined above and must therefore likewise be declared admissible.

B. Merits

1. The parties' submissions

49. The applicant submitted that the only evidence on which the domestic courts had relied in finding her guilty had been the content of her email messages, which had been obtained unlawfully.

50. The Government argued that the content of the email correspondence had been obtained lawfully. They pointed out that, if the Court were to take a different view, the admission of unlawfully obtained evidence did not automatically entail a violation of the right to a fair trial. The Government emphasised that the applicant's conviction had been based on a substantial and consistent body of evidence and not solely on the content of her email correspondence. Moreover, since the evidence in question was strong and its reliability was not disputed by the applicant, the need for corroborating evidence was correspondingly weaker. The Government also underlined the public interest in prosecuting tax offences and stressed that the applicant's defence rights had been respected.

2. *The Court's assessment*

(a) General principles

51. The Court reiterates that, while Article 6 of the Convention guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence as such, which is primarily a matter for regulation under national law. It is therefore not the role of the Court to determine, as a matter of principle, whether particular types of evidence – for example, evidence obtained unlawfully in terms of domestic law – may be admissible or, indeed, whether the applicant was guilty or not. The question which must be answered is whether the proceedings as a whole, including the way in which the evidence was obtained, were fair. This involves an examination of the "unlawfulness" in question and, where a violation of another Convention right is concerned, the nature of the violation found (see *Jalloh v. Germany* [GC], no. 54810/00, §§ 94-95, ECHR 2006-IX, and *Bykov v. Russia* [GC], cited above, §§ 88-89).

52. In determining whether the proceedings as a whole were fair, regard must also be had to whether the rights of the defence were respected. It must be examined in particular whether the applicant was given the opportunity of challenging the authenticity of the evidence and of opposing its use. In addition, the quality of the evidence must be taken into consideration, including whether the circumstances in which it was obtained cast doubts on its reliability or accuracy. While no problem of fairness necessarily arises where the evidence obtained was unsupported by other material, it may be noted that where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker (see *Jalloh*, cited above, § 96, and *Bykov*, cited above, § 90). In this connection, the Court further attaches weight to whether the evidence in question was or was not decisive for the outcome of the proceedings (see *Gäfgen v. Germany* [GC], no. 22978/05, § 164, 1 June 2010).

53. The Court has previously found in the particular circumstances of various cases that the fact that domestic courts had used evidence which had been deemed to have been unlawfully obtained for the purposes of Article 8 did not conflict with the requirements of fairness enshrined in Article 6 of the Convention (see, among other authorities, *Khan v. the United Kingdom*, no. 35394/97, §§ 34-40, ECHR 2000-V; *P.G. and J.H. v. the United Kingdom*, no. 44787/98, §§ 76-81, 25 September 2001, ECHR 2001-IX; and *Dragoş Ioan Rusu v. Romania*, no. 22767/08, §§ 51-57, 31 October 2017).

(b) Application of those principles to the circumstances of the present case

54. The Court would observe at the outset that while the evidence at issue was not obtained in accordance with the law within the meaning of Article 8 of the Convention (see paragraph 44 above), its use by the domestic courts does not automatically entail a violation of Article 6 of the Convention (unlike the admission of evidence obtained in breach of Article 3 of the Convention, which always raises serious issues as to the fairness of the proceedings – see *Gäfgen*, cited above, §§ 166-67, and *El Haski v. Belgium*, no. 649/08, § 85, 25 September 2012). In this connection, the Court would point out that there is nothing to suggest that the police, who had obtained judicial authorisation prior to procuring the content of the applicant's email communications, acted in bad faith or in intentional breach of formal rules when obtaining and executing that order (see, *mutatis mutandis*, *Prade v. Germany*, no. 7215/10, § 37, 3 March 2016). The unlawfulness in the present case related rather to the content of the order addressed to the communications service provider and

the inconsistent and unforeseeable approach taken by the domestic courts when reviewing the order in the criminal proceedings (see paragraph 43 above).

55. The Court further notes that the applicant had an effective opportunity to oppose the use of the evidence in question, and that she used that opportunity during the proceedings before four levels of domestic courts, all of which duly considered her complaints. The fact that the applicant was unsuccessful at each level is not decisive in this respect (see *Khan*, cited above, § 38, and *Dragojević v. Croatia*, cited above, § 132).

56. As regards the quality of that evidence, the Court observes that the applicant did not put forward any arguments disputing the authenticity of the emails obtained by the police. Instead, she confined her complaints to the manner in which the evidence had been obtained and its subsequent use. It is therefore undisputed between the parties that the applicant was the author of the messages that had been forwarded to Omissis's mailbox, frow which they were obtained. There is therefore nothing to cast doubt on the reliability or accuracy of that evidence.

57. As regards the importance of the disputed evidence, the Government contended that the content of the email communications was crucial but not the only incriminating evidence against the applicant. While the Court acknowledges that the domestic courts assessed a complex body of evidence concerning a large number of defendants, it finds it clear from the reasoning of their decisions, in particular that delivered by the first-instance court, that it was the content of the applicant's email messages that had made it possible to prove that the invoices and leasing agreements were fictitious. It therefore appears that the content of the applicant's emails had indeed been decisive evidence for the outcome of the criminal proceedings against her. However, the Court reiterates that where the evidence is strong and there is no risk of its being unreliable, as in the present case, the need for supporting evidence is correspondingly weaker. Indeed, the fact that an applicant was convicted on the basis of a single but reliable piece of evidence, although obtained unlawfully and, as such, contested by him or her, is not in itself contrary to the requirement of a fair trial (see *Prade*, cited above, § 40).

58. Lastly, in determining whether the proceedings as a whole have been fair, having regard, on one hand, to the manner in which the offenders operated and the applicant's involvement, and, on the other hand, to the relatively mild interference with the applicant's rights under Article 8 (see paragraph 34 above) and the fact that her defence rights were duly respected, the Court finds that the overall fairness of the trial was not irretrievably prejudiced by the admission of the contested evidence.

59. It follows that there has been no violation of Article 6 § 1 of the Convention.

III. OTHER ALLEGED VIOLATIONS OF THE CONVENTION

60. Lastly, the applicant complained under Article 13 of the Convention that the Constitutional Court had not taken the Court's case-law into account and, consequently, had failed to protect her fundamental rights.

61. The Court is of the view that the applicant's complaint can be considered as aimed at the outcome of the investigation in the present case and that, as such, it amounts to a restatement of her complaints under Articles 6 and 8 of the Convention. For this reason, it concludes that, while this complaint is admissible, no separate issue arises under Article 13 of the Convention.

IV. APPLICATION OF ARTICLE 41 OF THE CONVENTION

62. 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

63. The applicant claimed 50,000 Czech crowns (CZK) (approx. 2,000 euros (EUR)) in respect of pecuniary damage, corresponding to the amount of the financial penalty imposed on her in the criminal proceedings. She also claimed CZK 200,000 (approx. EUR 8,150) in respect of non-pecuniarydamage, on account of the outcome of the criminal proceedings and the sentence imposed, and on account of the manner in which her right to privacy had been infringed.

64. As to pecuniary damage, the Government pointed out that, in the event of the finding of a violation, the applicant would have the possibility to request the reopening of the criminal proceedings. As to non-pecuniary damage, they did not see any causal link between the damage claimed by the applicant and the alleged violation of the Convention.

65. The Court does not discern any causal link between the violation found and the pecuniary damage alleged; it therefore rejects this claim. Furthermore, having regard to all the circumstances of the present case, the Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage caused to the applicant (see *Roman Zakharov*, cited above, § 312).

B. Costs and expenses

66. The applicant also claimed CZK 188,493 (approx. EUR 7,700) for the costs and expenses incurred before the domestic courts and the Court.

67. The Government observed that the applicant had submitted only a contract entered into between her and her lawyer for the legal assistance to be provided before the Constitutional Court and the Court, in which they agreed on a fee of CZK 2,000 (EUR 80) per hour, but no itemised bills or invoices.

68. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 2,500 covering costs under all heads, plus any tax that may be chargeable to the applicant.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;
2. *Holds* that there has been a violation of Article 8 of the Convention;
3. *Holds* that there has been no violation of Article 6 § 1 of the Convention;

4. *Holds* that no separate issue arises under Article 13 in conjunction with Articles 6 § 1 and 8 of the Convention;

5. *Holds* that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant;

6. *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, EUR 2,500 (two thousand five hundred euros), to be converted into the currency of the respondent State at the rate applicable at the date of settlement, plus any tax that may be chargeable to the applicant, in respect of costs and expenses;

   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

7. *Dismisses*, unanimously, the remainder of the applicant's claim for just satisfaction.

   Done in English, and notified in writing on 13 February 2025, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

   Victor Soloveytchik Registrar

   Mattias Guyomar President