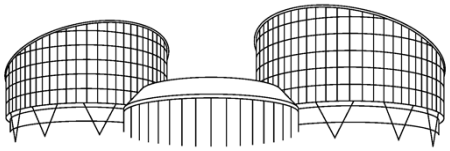

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIRST SECTION

CASE OF ŠKOBERNE v. SLOVENIA

(Application no. 19920/20)

JUDGMENT

Art 6 § 1 (criminal) and Art 6 § 3 (d) • Fair hearing • Trial judge's refusal of applicant's request to examine two co-defendants as witnesses following their admission of guilt rendered trial proceedings unfair • Request for examination of co-defendants essentially meant to support the applicant's defence, sufficiently founded and relevant to the subject-matter of the accusations against him • Co-defendants' testimony could be considered as being capable of influencing the outcome of the trial or strengthening the position of the defence • Applicant deprived of the opportunity to effectively adduce and thus rely on witness evidence in arguing his case • Domestic courts' failure to provide sufficient reasons for refusal and redress resulting shortcomings
Art 8 • Private life • Correspondence • Applicant's telecommunications data (traffic and location data) retained by telecommunications providers for statutory period of 14 months for different public interest purposes, accessed by law-enforcement authorities and used in criminal proceedings against him • Systemic surveillance entailed by the mandatory retention of telecommunications data presented an impediment to the enjoyment of privacy rights of all users of telecommunication services • Interference constituted by data retention of a serious nature requiring the Court to exercise stricter scrutiny in assessing the question of fair balance • Absence of provisions or mechanisms aimed at ensuring impugned retention measure limited to what was "necessary in a democratic society" to achieve specific purposes listed in the relevant domestic law • Applicant's data at the time retained in a systemic, general and indiscriminate manner • Retention regime irreconcilable with State's Art 8 obligations; access to and use of such data likewise noncompliant with that provision

STRASBOURG

15 February 2024

In the case of Škoberne v. Slovenia,

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

Alena Poláčková*, President*,
Marko Bošnjak,
Lətif Hüseynov,
Péter Paczolay,
Ivana Jelić,
Erik Wennerström,
Raffaele Sabato*, judges*,

and Liv Tigerstedt, *Deputy Section Registrar,*

Having regard to:

the application (no. 19920/20) against the Republic of Slovenia lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Slovenian national, Mr Milko Škoberne ("the applicant"), on 21 April 2020;

the decision to give notice to the Slovenian Government ("the Government") of the complaints concerning Article 6 (with respect to the trial judge's impartiality and her refusal to allow the examination of E.R. and M.S. as witnesses at the applicant's trial) and Article 8 of the Convention and to declare inadmissible the remainder of the application;

the parties' observations;

Having deliberated in private on 23 January 2024,

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

INTRODUCTION

1. The case concerns criminal proceedings against the applicant (a former district court judge) in which he was convicted of accepting bribes by a judge who had previously accepted the admission of guilt made by his two co-defendants. The applicant was denied the possibility to examine those co-defendants as witnesses following their admission of guilt. The case also concerns a question whether Article 8 was breached because the applicant's traffic and location data was – as part of a systemic measure – retained for a period of 14 months and used by the authorities in the proceedings against him.

THE FACTS

2. The applicant was born in 1959 and lives in Laško. The applicant was represented by Mr V. Cugmas, a lawyer practising in the town of Slovenske Konjice.

3. The Government were represented by their Agent, Mrs A. Grum, Senior State Attorney.

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

I. EVENTS LEADING TO THE CRIMINAL PROCEEDINGS AGAINST THE APPLICANT

5. E.Ć. was convicted in 2001 before Celje District Court for the criminal offence of fraud and sentenced to imprisonment for two years. He then left the territory of Slovenia before his prison sentence had begun; an international arrest warrant against him was issued on 12 December 2007 ("the 2007 arrest warrant"). On 5 November 2008 the enforcement of the sentence became statute-barred. On that day the 2007 arrest warrant was revoked.

6. Simultaneously, another set of criminal proceedings against E.Ć. took place before the Celje District Court concerning a prostitution-related crime. His detention was ordered on 3 December 2003. On 28 May 2009 the Celje District Court issued an international arrest warrant against E.Ć. ("the 2009 arrest warrant").

7. On 10 October 2009 E.Ć. was detained on the basis of the 2009 arrest warrant by the Croatian enforcement authorities when he tried to cross the border from Croatia to Bosnia and Herzegovina. However, he was quickly thereafter released. The applicant was on that day serving as an on-duty investigating judge at the Celje District Court.

8. In April 2010 E.Ć. lodged with the Celje District Court written submissions requesting that certain evidence be removed from the case file and that the criminal proceedings against him be suspended.

9. On 12 November 2010, at E.Ć.'s written request (which was supported by a statement given by him and by certain medical certificates relating to the health of the woman who, he asserted, was his partner), an out-of-court panel of three judges – which was chaired by the applicant – decided to suspend E.Ć.'s detention. On the same day, the applicant issued a decision revoking the 2009 arrest warrant issued against E.Ć.

10. On 29 November 2010 E.Ć. lodged via email a criminal complaint against the applicant with the police. He lodged another complaint (providing further details) orally at a police station on 14 December 2010. He alleged that the applicant (with the assistance of two intermediaries – M.S. and E.R.) had committed the criminal offence of accepting a bribe, describing the events as follows. Following arrangements made by E.R. and M.S., he had met with the applicant, who had declared himself to be potentially willing to help him in respect of the proceedings pending against him and in respect of the related arrest warrants (see paragraphs 5 and 6 above). After the first meeting (which had been held in Croatia at the end of 2008 or the beginning of 2009, and at which the applicant had promised to look into the matter), E.Ć. had met the applicant again in the spring of 2009. E.R. and M.S. had also been present. At that meeting the applicant had informed E.Ć. that the

2007 arrest warrant had been revoked (see paragraph 5 above) but that a new arrest warrant (that is, the 2009 arrest warrant – see paragraph 6 above) had been issued against him; the applicant had then demanded payment for his favours. E.Ć. had given 5,000 euros (EUR) to E.R. (to be handed on to the applicant). A third meeting had been held in the summer of 2009, involving the same persons as before. E.Ć. had given EUR 4,000 to E.R. (to be handed on to the applicant). The applicant had prepared a written submission (which E.Ć. had then lodged with the Celje District Court – see paragraph 8 above) and had promised to try to have E.Ć.'s case transferred to himself. Following the suspension of E.Ć.'s detention and the revocation of the 2009 arrest warrant (see paragraph 9 above), the applicant had demanded a further EUR 50,000 for his favours and had threatened that otherwise a new arrest warrant would be issued against E.Ć.

11. Together with his criminal complaint, E.Ć. submitted to the police several items of evidence and provided details concerning the telephone numbers used for communication between the participants during the above-noted events.

II. DATA-GATHERING, SURVEILLANCE AND UNDERCOVER OPERATION

12. On 16 December 2010 the Ljubljana District Court ordered the relevant telecommunications service providers to provide traffic and location data and related subscriber data (hereinafter "telecommunications data") in respect of the telephone numbers that had been used by, *inter alia*, E.Ć. and E.R. concerning the period of 1 January 2009 to 16 December 2010. Based on the data received from the telecommunications service providers (see paragraph 17 below) the police, on 18 December 2010, prepared an analytical report establishing, *inter alia*, that E.R. during the period in question had engaged in communication with a person using a mobile telephone number belonging to the Celje District Court. On 20 December 2010 the police prepared a second analytical report on the basis of the same order; that report set out the telecommunications data detailing communication between E.R.'s and M.S.'s respective telephone numbers.

13. On 18 December 2010 the Ljubljana District Court ordered a measure of surveillance of telecommunications (*nadzor telekomunikacij*) – namely, it ordered the wiretapping of several telephone numbers used by E.R. and the recording of communication obtained thereby.

14. On 23 December 2010 the Ljubljana District Court ordered the relevant telecommunications service providers to provide it with the telecommunications data in respect of telephone numbers used by, *inter alia*, E.R. and M.S. concerning the period of 1 January 2009 to 22 December 2010. Based on the data received from the telecommunications service providers (see paragraph 17 below) pursuant to the Ljubljana District Court's orders of

16 December and 23 December 2010 the police prepared a third analytical report on 27 December 2010. That report set out the telecommunications data relating to E.R. and M.S. and a mobile telephone number that belonged to the Celje District Court.

15. On 27 December 2010 the Ljubljana District Court ordered a measure of surveillance of telecommunications – namely, it ordered the wiretapping of the mobile telephone number of the Celje District Court (which was used by the applicant) and of a landline telephone number owned and used by the applicant, and the recording of communication obtained thereby.

16. On 12 January 2011 the Ljubljana District Court ordered telecommunications service providers to provide telecommunications data in respect of a mobile telephone number that belonged to the Celje District Court and was used by the applicant. On 17 January 2011 the police prepared a fourth analytical report on the basis of the data supplied by the telecommunications service providers (see paragraph 17 below) pursuant to the Ljubljana District Court's orders of 16 December, 23 December 2010 and 12 January 2011. That report set out, *inter alia*, the telecommunications data relating to the traffic between the telephones used by the applicant, E.R. and M.S.

17. In reply to the above-mentioned orders issued by the Ljubljana District Court for the telecommunications service providers to yield the requested telecommunications data, the telecommunications service providers explained that they could not provide the solicited information in respect of the entire period but only in respect of the previous fourteen months – the minimum storage period provided by the relevant legislation.

18. During and after the period during which the above-mentioned activities took place, an undercover operation was set up (in cooperation with E.Ć.). An undercover police officer and E.Ć. engaged in operations that were targeted at E.R., M.S. and the applicant until 18 February 2011. E.Ć. engaged in communication and participated in meetings held in Slovenia with the aforementioned persons. On 24 January 2011, he delivered to E.R. and M.S. banknotes (whose serial numbers had been recorded) in the amount of EUR 18,000. During subsequent house searches, some of those banknotes were recovered at premises of E.R. and M.S.; on 25 January 2011 the applicant deposited in a bank cash (in the amount of EUR 8,000) comprising more of the above-mentioned banknotes. During the search of the applicant's house, his IT equipment was seized. Documents containing the submissions lodged with the Celje District Court by E.Ć. in April 2010 (see paragraph 8 above) were found on the hard disk of his computer.

19. The applicant, E.R. and M.S. were arrested on 26 January 2011.

III. CRIMINAL INVESTIGATION LED BY THE INVESTIGATING JUDGE

20. On 28 January 2011 the applicant, E.R. and M.S. appeared before the investigating judge. The applicant declined to give any statement. E.R. remained silent. M.S. gave a statement in the presence of his lawyer.

21. In his statement, M.S. said that in 2009 E.R. had asked him if he had known a legal expert who could help his acquaintance – E.Ć. – with certain legal issues. M.S. had known the applicant because they had been school friends, so he had given E.R. his telephone number. E.R. had then contacted the applicant directly. M.S. acknowledged having met E.Ć., E.R. and the applicant in Croatia as well as having received, on the day of the incident at the border crossing (see paragraph 7 above), a telephone call from E.Ć. during which the latter had asked how he could reach the applicant and had referred to certain complications that he was experiencing at a border crossing. He further explained that on 24 January 2011 (see paragraph 18 above) he, E.R. and E.Ć. had met up. He had received from E.Ć. an envelope containing EUR 18,000 in cash and had then divided that cash between three envelopes (two containing EUR 5,000 and one containing the amount of EUR 8,000). Later that day, he had met the applicant and handed to him the envelope containing EUR 8,000. Together with the applicant, he had then met E.R. and E.Ć. in a hotel in the same town. They had discussed the fact that the hearing in respect of E.Ć.'s case (see paragraph 6 above) had been postponed owing to the illness of the judge or the prosecutor. When leaving the hotel, M.S. had given one of the envelopes containing EUR 5,000 to E.R.

22. On 3 February 2011, the investigating judge opened an investigation against the applicant, E.R. and M.S. During the investigation E.Ć. was interviewed as a witness.

23. On 10 January 2012 the State Prosecutor's Office filed a bill of indictment against the applicant, E.R. and M.S. for committing the criminal offence of accepting bribes. Requests lodged by the applicant for the exclusion of certain evidence, as well as the objections lodged by the applicant, E.R. and M.S. against the indictment, were dismissed. In lodging those requests and complaints, the applicant did not refer to the storage of telecommunications data by the telecommunications service providers in question and the use of such data as evidence.

IV. TRIAL BEFORE THE LJUBLJANA DISTRICT COURT

24. On 22 November and 20 December 2012, the Ljubljana District Court, sitting as a single judge (Judge V.L.), held pre-trial hearings of the applicant, E.R. and M.S., respectively. Their lawyers lodged requests for the exclusion of certain evidence but did not question the lawfulness of the data storage by telecommunication service providers.

25. On 14 February 2013 the trial commenced before Judge V.L. of the Ljubljana District Court. At the first hearing, the applicant stated that he would provide a defence statement – but only at a later stage of the proceedings. M.S. also stated that he would defend himself later. E.R. likewise did not defend himself. The court read out the statement that M.S. had given during the investigation (see paragraph 21 above). The applicant then commented on that statement. He argued that M.S. had not been asked whether the applicant had known of the demands made on his behalf, and had not been questioned as to why he had given the applicant EUR 8,000. The applicant also alleged that no enquiries had been made with M.S. as to whether he and the applicant had been involved in some other kind of relationship or business.

26. A number of further hearings were held between 21 February 2013 and 5 December 2013, during which extensive evidence was taken – including the playing of wiretap recordings and the examination of several witnesses who had been involved directly or indirectly in the events in question. E.Ć. was also examined as a witness, and (as had not been the case during his previous submissions during the criminal-complaint proceedings and investigation) he now testified that the money – which he had given to E.R. and which the latter had said he had passed on to the applicant – had been meant as a payment for legal services and not as a bribe. He said that he had also given that information to the police when lodging his criminal complaint on 14 December 2010 (see paragraph 10 above), but that it had been left out of the record thereof. He also gave his account of the events on the Croatian-Bosnian border (see paragraph 7 above), stating, *inter alia*, that he had shown the border guards a document concerning the (revoked) 2007 arrest warrant, which had been given to him by the applicant, but that that had not yielded the desired results – prompting his partner to then call E.R. Thirty or forty minutes later he had been released. E.Ć. also submitted that E.R. had on the day after the incident told him that he had been lucky that the applicant had been on duty that day and that he had been able to "save" him. He further testified that after the 2009 arrest warrant had been revoked and the detention order suspended, E.R. had demanded a payment of EUR 50,000; E.R. had reduced his demand to EUR 40,000 following negotiations involving M.S. He further described his subsequent cooperation with the police. The police had tasked him with negotiating the payment and had instructed him to hand over the agreed sum of money on condition that the applicant agreed to meeting him. He had paid the sum and on the evening of the same day he had met with the applicant, together with M.S. and E.R. (see paragraph 18 above). During his examination, E.Ć. also replied to questions posed by the applicant or his representative. He said that the money (EUR 9,000) which he had given to E.R. and which the latter had said that he had handed on to the applicant had been – in his understanding – intended as payment for legal services or for "lawyers". He also testified that he had several times turned to the

applicant, via M.S. and E.R., for advice regarding the proceedings pending against him.

27. At a hearing on 11 December 2013 M.S. and E.R. pleaded guilty to the charges. Judge V.L. accepted their admission of guilt and accordingly found them guilty (see paragraph 35 below). The applicant then lodged an application seeking the recusal of Judge V.L. on the grounds that there were doubts concerning her impartiality. The president of the Ljubljana District Court dismissed the applicant's application. He noted that the Criminal Procedure Act (hereinafter "the CPA") did not provide that a judge should step down in the event that he or she accepted the co-defendants' admission of guilt. Rather, the CPA only provided (in its section 39(2)(3) – see paragraph 56 below) that a judge or a juror could not adjudicate an indictment, appeal or extraordinary legal remedy if he or she had delivered a decision rejecting a defendant's admission of guilt or an agreement concerning a defendant's admission of guilt. Pursuant to the presumption of innocence, the court in question had to determine guilt separately for each defendant. He further explained that for the recusal of a judge on the basis of section 39(1)(6) of the CPA (see paragraph 56 below), there should be circumstances raising doubts about the judge's impartiality.

28. On 13 December 2013 the court disjoined the proceedings against E.R. and M.S. from those against the applicant (see paragraphs 35-36 below).

29. At the hearing on 13 and 19 December 2013, the applicant gave defence statements. The applicant explained that he had met E.Ć. for the first time in Croatia on 17 November 2008 at the initiative of M.S., who had been a school friend of the applicant. He confirmed that when the meeting had been held he had been aware that criminal proceedings against E.Ć. had been pending. According to the applicant, E.R. (whom the applicant had not known) had also been present at the meeting as a long-time friend of E.Ć. He further stated that he had explained to E.Ć. that he was entitled to the services of a state-appointed lawyer but that if he was not satisfied with that lawyer, he could choose his own (however, he would have to pay for the services of the lawyer of his own choice). The applicant stated that the subject of money had not been discussed – either then or later. In respect of a further meeting that he had had with E.Ć., M.S. and E.R., the applicant stated that M.S. had done most of the talking. The applicant submitted that M.S. had asked what he would have done if he had been the judge in E.Ć.'s case. The applicant said that he had replied that he would have probably suspended the proceedings but that he could not take over E.Ć.'s case because he had been involved at an earlier stage and that for the case to be reallocated, certain conditions would have to be met.

30. With regard to the event that had taken place on 10 October 2009 at the border crossing between Croatia and Bosnia and Hercegovina (see paragraph 7 above), the applicant stated that M.S. had told him that E.Ć. had been "detained at a border crossing between Bosnia and Croatia" and had

later telephoned again to say that he had been released. According to the applicant, when he had told M.S. that he had been on duty on the day in question M.S. had replied: "You must have sorted it out because you [were] on duty." The applicant stated that that information had obviously been passed on to E.Ć.

31. With regard to money, the applicant stated that he had not received the EUR 9,000 that had been handed over to E.Ć. There had been no talk of money at the meetings. Regarding his receipt of the above-mentioned sum of EUR 8,000, the applicant stated that that money had been given to him in repayment of money that he had loaned to M.S. in July 2010.

32. At the hearing on 19 December 2013 the applicant's lawyer requested that E.R. and M.S. be examined. He argued, *inter alia*, that M.S. could provide information concerning the alleged loan that the applicant had mentioned in his defence statement, and that E.R. could testify in respect of E.Ć.'s alleged debts to him. Moreover, the applicant's lawyer submitted that E.R. and M.S. had not told the applicant that they had requested money on his behalf and should explain the circumstances surrounding the question of that money, what had happened to the initial EUR 9,000, and how and why the sum of EUR 18,000 had been divided. The applicant's lawyer also pointed out that E.R. and M.S. were no longer co-defendants in the same proceedings and could therefore be examined as witnesses in the proceedings against the applicant. According to the applicant's lawyer, following their admission of guilt and their conviction, E.R. and M.S. had become incriminating witnesses (that is, witnesses testifying against the accused); the applicant was unable to put questions to M.S. (who had given incriminating testimony against the applicant and had later decided to not defend himself) or to examine E.R. (who was absent).

33. At the hearing on 19 December 2013 Judge V.L. refused the request lodged by the applicant's lawyer that the examination of E.R. and M.S. be permitted; the judge reasoned that both persons still had the status of defendants because the judgment against them had not yet become final. She stated that sufficient evidence had been presented to allow a decision to be delivered in respect of the charges against the applicant. She added that it was impossible to clarify with E.R. and M.S. the reason or motive for their respective admissions of guilt because that would have infringed their legal rights.

34. The applicant subsequently repeated his request that E.R. and M.S. be examined, arguing that the hearing should be postponed until the judgment against E.R. and M.S. was final and submitting that such an examination would yield the most important evidence for his defence. Judge V.L. again refused the request. In the judgment against the applicant (see paragraph 37 below) she put forward two grounds. Firstly, she held that at the time when the application requesting that E.R. and M.S. be examined had been under consideration, the judgment against E.R. and M.S. had not yet been final, and

it had not been certain that it would become final after the expiry of the deadline for declaring an intention to appeal. According to the relevant domestic case-law, co-defendants – even when tried in separate proceedings – could not be examined as witnesses in proceedings against other co-defendants, unless the judgment against them was final. Secondly, the judge held that the questioning of co-defendants could not have a decisive effect on its assessment of evidence that had already been examined. She noted that the court had not based its assessment of the evidence presented to it on the fact that E.R. and M.S. had admitted their guilt nor on the statement given by M.S. (which had been read out during the trial). She further noted that even if M.S. had not defended himself before the investigating judge and the admission of guilt by E.R. and M.S. had not been accepted, she would have convicted the applicant on the basis of numerous items of evidence collected independently of the admission of guilt. The judge further noted that the applicant had been able to submit comments regarding the statement (containing some incriminating assertions) given by M.S. during the investigation, and found that the applicant's late-stage defence was unpersuasive and that he could have submitted relevant evidence at an earlier stage of the proceedings.

V. JUDGMENT AGAINST E.R. AND M.S.

35. On 16 December 2013 Judge V.L. convicted E.R. and M.S. on the basis of their respective admissions of guilt, imposing on them a suspended prison sentence and a fine of approximately EUR 3,000 each. They were found guilty of the continuous offence of accepting a bribe for the purpose of "assisting in the bribery of an official who demanded and accepted a reward for abusing his position". The judgment further stated that E.R. and M.S. had each assisted in "the bribery of an official, Judge Milka Škoberneta", and outlined the following acts, by means of which the said criminal offence had been committed:

- E.R. and M.S. had arranged three meetings with E.Ć. and the applicant in 2009.
- E.R. had demanded and received, in the applicant's name, EUR 9,000 from E.Ć.
- E.R. and M.S. had informed the applicant of the incident at the border crossing involving E.Ć. (see paragraph 7 above), after which the applicant – as the investigating judge on duty at the Celje District Court on the day in question – had interfered by sending a decision revoking the 2007 arrest warrant (which in fact had been irrelevant to the situation in question), thereby securing E.Ć.'s release.
- E.R. had intervened in such a way (*posreduje pri*) that the applicant had prepared written submissions for E.Ć. to lodge with the Celje District Court which had been through his facilitation placed in the case file (see paragraph

8 above); moreover, E.R. had transferred to E.Ć. certain submissions prepared by the applicant that had been designed to facilitate the taking of a decision to suspend E.Ć.'s detention and the revocation of the 2009 arrest warrant (see paragraph 9 above); furthermore, E.R. had intervened to ensure that E.Ć. signed the submission and had acquired evidence requested by the applicant (which E.R. had known was misleading in nature).

- E.R. and M.S. had demanded EUR 50,000, and later EUR 40,000, from E.Ć. with the aim of obtaining a reward for the applicant and for their assistance, which they had discussed by telephone and at the meetings with E.Ć. (of which they had kept the applicant informed).

- E.R. and M.S. had received, for themselves and for the applicant, a bribe from E.Ć. in the amount of EUR 18,000.

36. The judgment against M.S. and E.R. had become final on 25 December 2013 after the expiration of an eight-day deadline before which E.R. and M.S. could have (but had not) declared their intention to appeal.

VI. JUDGMENTS AGAINST THE APPLICANT

A. The Ljubljana District Court's judgment

37. On 23 December 2013 Judge V.L. of the Ljubljana District Court, found the applicant guilty of the continuous offence of accepting a bribe (Judge V.L. having deemed that the applicant, as a district judge at the Celje District Court – and thus an official – had demanded and accepted a reward for abusing his position while exercising his official powers).

38. Judge V.L. found, i*nter alia*, that the applicant had: promised E.Ć. that he would try to take over the hearing of his case (see paragraph 6 above) and to terminate the proceedings against him; promised E.Ć. that he would try to have the 2009 arrest warrant (see paragraph 6 above) revoked; prepared the written submissions for E.Ć. that had been lodged in April 2010 (see paragraph 8 above); intervened (in his role as duty investigating judge) to secure E.Ć.'s release at the Croatia-Bosnia border crossing (see paragraph 7 above) by sending a decision – which he had known did not concern the arrest warrant that had served as the grounds for E.Ć.'s detention (the 2009 arrest warrant) but rather concerned the (revoked) 2007 arrest warrant; and presided over the out-of-court panel that had suspended E.Ć.'s detention and had subsequently revoked the arrest warrant on the basis of a written request and other documents that had been prepared on behalf of E.Ć. or been solicited by the applicant (who had known that the information contained therein was inaccurate – see paragraph 9 above). Judge V.L. established that as a reward for the above-noted actions the applicant – with the assistance of E.R. and M.S. and together with them – had demanded and received EUR 9,000 from E.Ć. at some point between November 2008 and June 2009. It further found that the applicant – together with E.R. and M.S. – had subsequently demanded

EUR 50,000 or EUR 40,000 at some point between 14 November 2010 and 24 January 2011, of which he – together with E.R. and M.S. – had received EUR 18,000 on 24 January 2011.

39. In reaching those findings the court referred to E.Ć.'s statements to the police in which he had described the meetings that had taken place in Croatia; it found those statements to have been corroborated by the statement that M.S. had made during the investigation (see paragraphs 10 and 21 above). It also referred to the telecommunications data that had been provided by the relevant telecommunications service providers and had been analysed by the police (see paragraphs 12, 14 and 16 above) which, in the court's opinion, had corroborated the evidence given initially by E.Ć. In particular, it referred to the analysis showing that communication had taken place involving E.R., M.S., E.Ć. and the applicant on the day of the above-mentioned incident at the border crossing (see paragraph 7 above) and to the out-of-court panel's decision regarding E.Ć.'s detention (see paragraph 9 above). As regards the finding that the applicant had promised to tamper with the legal process in respect of E.Ć. (with the expectation of receiving payment by way of reward), the court referred also to the communications recorded by means of wiretapping and to the results of the undercover operation. For instance, in one of the conversations M.S. had been recorded saying that E.Ć. had given EUR 9,000, thinking that the matter had been resolved. During the meeting on 24 January 2011 the applicant had been recorded explaining that he had been on duty on the day of the border crossing incident (see paragraph 7 above) and that he had sent the revoked 2007 arrest warrant. As regards that incident the court also referred to M.S.'s statement (see paragraph 21 above) in which he had said that E.R. had called him that day asking how he could reach the applicant.

40. As regards the events following the suspension of E.Ć.'s detention and the revocation of the 2009 arrest warrant (see paragraph 9 above), the court referred to, *inter alia*, the following evidence. On several occasions M.S. and E.R. had been recorded discussing the progress of the criminal proceedings against E.Ć. (see paragraph 6 above) and their frustrations regarding E.Ć.'s failure to pay the requested sums. They had often mentioned the applicant as someone who had been consulted during or involved in the discussions of E.Ć.'s criminal case. The records of the conversations between E.R. and the applicant showed that E.R. (while at a meeting on 31 December 2010 with E.Ć.) had telephoned the applicant and had informed him that "things [were] moving in a slightly better direction". The court also referred to a number of recorded conversations between E.R. and E.Ć. in which the former had asked E.Ć. to pay, whereupon the latter (who had been acting as part of the undercover operation) had insisted on a meeting with the applicant. The record of a subsequent conversation that had taken place between M.S. and the applicant on 7 January 2011 showed that M.S. had informed the applicant that "he" had wanted to meet with him, to which the applicant had agreed. At

a meeting on 8 January 2011 between E.R., E.Ć. and M.S., the latter had said that the applicant could not meet publicly with the defendants, and that they could not "play" with that. The court referred also to subsequent conversations between the applicant and M.S. in which the latter had been recorded saying that "he" was still bargaining and wanted to meet the applicant and that "he" was softening up. During one of those conversations reference had also been made to events that had occurred during the criminal proceedings that had seemingly related to E.Ć. At the above-mentioned meeting on 24 January 2011 (see paragraph 18 above) the applicant had been recorded saying in response to E.Ć. (who had been explaining the difficulties encountered in collecting the money) that those difficulties were not a problem. As for the division of the money handed over on 24 January 2011, the court referred to M.S.'s statement (see paragraph 21 above) and the record of a conversation between E.R. and M.S. in which the latter had proposed that the money be divided according to the ratio of "5,5,8".

41. In the court's view, the recorded conversations indicated that the applicant had known of the required payment and its purpose. It thus found the applicant's statement to the effect that the money received from M.S. had constituted the repayment of a loan (see paragraph 29 above) to have constituted "merely his means of defence". In that connection, the court also noted that the applicant had failed to convincingly demonstrate how he had obtained the money at the time when he had allegedly given it to M.S. As regards the change to E.Ć.'s testimony, the court noted that his statements at the trial (see paragraph 26 above) had lacked credibility and that he could have been also influenced by threats that he had received during the proceedings.

42. The applicant was sentenced to five years and six months in prison and a fine of almost EUR 20,000; he was also ordered to pay EUR 12,000 – a sum that amounted to the pecuniary gain realised from the crime committed.

B. The Ljubljana Higher Court's judgment

43. The applicant appealed against the first-instance court's judgment on the grounds that E.R. and M.S. had not been examined and that Judge V.L. had not stepped down, despite her having accepted E.R.'s and M.S.'s admissions of guilt. The applicant submitted that he had never demanded or received money from E.Ć., and that by handing him EUR 8,000, M.S. had merely been repaying a loan. He also alleged that the first-instance court, in convicting the applicant and in substantiating orders for obtaining other evidence, had relied on telecommunications data which had been retained under a legal regime which had been declared invalid and which had been in violation of, *inter alia*, Article 8 of the Convention. In that connection, he relied on the Constitutional Court's judgment of 3 July 2014 and the judgment delivered by the Court of Justice of the European Union (CJEU) in the case

of *Digital Rights Ireland and Others* (see paragraphs 66-68 and 74-76 below) and pointed out the indiscriminate and general nature of the data-retention regime in question.

44. In a judgment of 22 September 2014, the Ljubljana Higher Court dismissed the applicant's appeal and upheld the findings of the Ljubljana District Court. As concerns the refusal of the request that E.R. and M.S., be examined, the Ljubljana Higher Court found that it was not disputed that E.R. and M.S. could not be examined as witnesses until the moment at which the judgment against them became final. The judgment against the applicant had been delivered before that moment. The Ljubljana Higher Court also held that the applicant had failed to demonstrate with a sufficient degree of probability that any testimony that might have been given by E.R. and M.S. could have undermined the court's conclusions. With regard to the non-recusal of Judge V.L., the Ljubljana Higher Court held that the CPA did not provide that a judge should be recused in such a (by no means rare) procedural situation. It noted that before accepting the admissions of guilt, the court had had to assess whether the admissions were unambiguous and supported by the evidence in the case file (see paragraph 58 below).

45. As regards the gathering of data, the Ljubljana Higher Court noted that the Constitutional Court's decision had not interfered with section 149.b of the CPA (see paragraph 57 below) and had not instructed that the data that had been in possession of the authorities prior to its delivery be destroyed. Referring to the decision of the Constitutional Court (see paragraphs 66-68 below) and to the decision of the CJEU (see paragraphs 74-76 below), the Ljubljana Higher Court found that in the present case a sufficient level of suspicion (as stipulated by section 149.b of the CPA (see paragraph 57 below) that the applicant had been involved in a criminal offence had been established before the telecommunications data had been obtained and that that suspicion had later only intensified. The access orders had pertained to specific persons and to specific mobile telephones. Only one of four analytical reports produced by the police on the basis of the obtained telecommunications data (namely, the report dated 17 January 2011) had concerned the applicant. The number in question had been the telephone number of the Celje District Court (that is, a State institution) which diminished the severity of the alleged encroachment on the applicant's privacy. The Ljubljana Higher Court further reviewed the proportionality of the interference by taking into account the nature and severity of the corruption-related offences and concluded that the measures in question had been necessary.

C. The Supreme Court's judgment

46. The applicant lodged an application for the protection of legality, complaining, *inter alia*, that the first-instance court's refusal to allow the

examination of E.R. and M.S. had violated his Article 6 rights – including his right (under Article 6 § 3 (d)) to examine witnesses who had given evidence against him. The court could have postponed the hearing until the judgment against E.R. and M.S. became final. Article 6 had been violated also because Judge V.L. had not been recused from presiding over the proceedings before the first-instance court. The CPA, which did not provide that a judge had to step down in the event of such a procedural situation arising, contravened the Constitution. Furthermore – relying on (i) the Constitutional Court's decision of 3 July 2014, which had concerned provisions identical to those underpinning the retention of telecommunications data in his case, and (ii) the CJEU's judgment in *Digital Rights Ireland and Others* (see paragraphs 66-68 and 74-76 below) – the applicant argued that the retention and subsequent use of the telecommunications data had contravened the Convention, the Constitution and the relevant EU law and had, moreover, been disproportional. He submitted that – by assessing the legality of the authorities' retention of and access to the data in question – the Ljubljana Higher Court's judgment had contradicted the findings of the aforementioned courts. The applicant complained that he had been convicted on the basis of telecommunications data that had been obtained in violation of his privacy rights, and on the basis of evidence that had been yielded by that telecommunications data.

47. The applicant also pointed out that the Supreme Court in the disciplinary proceedings against him had found in its decision of 17 October 2014 that the retention regime provided by the Amended 2004 Act (see paragraph 64 below) – which had been identical to that provided by the 2012 Act (see paragraph 65 below) – had been unconstitutional. He also referred to the fact that the Supreme Court in those proceedings had excluded from the case file the analytical reports prepared on the basis of the retained telecommunications data and had instructed the lower court to establish the impact of those reports on the admissibility of related evidence.

48. On 9 June 2015 the Supreme Court dismissed the applicant's application for the protection of legality. With regard to the refusal of his request that E.R. and M.S. be examined, the Supreme Court followed the reasoning of the lower courts. It observed that at the time the request had been lodged it could have not been predicted that an appeal would not be lodged against E.R.'s and M.S.' conviction. The Supreme Court furthermore noted that the applicant had presented his defence (when he had raised new factual issues) only later in the proceedings.

49. The Supreme Court further pointed out that during the proceedings E.R. had not wished to defend himself and had invoked his right to remain silent. Concerning M.S., the defence had been informed of his testimony no later than by the start of the investigation on 3 February 2011 (see paragraph 22 above) but had nevertheless failed to request that he be examined during the trial. Irrespective of the foregoing, the first-instance court had not been

able to base its judgment exclusively or to a decisive extent on M.S.'s testimony.

50. With regard to the non-recusal of Judge V.L., the Supreme Court held that when the co-defendants had admitted their guilt just before the end of the taking of evidence, this in itself had not justified the recusal of a judge under section 39(1)(6) of the CPA (see paragraph 56 below). It agreed with the Ljubljana Higher Court that the legislature had obviously not considered a situation wherein a judge might reject an admission of guilt or a plea agreement comparable to the situation where he or she accepted it. It furthermore pointed out that a judge was required to decide – on the basis of the evidence – guilt and criminal sanctions in respect of each defendant separately, and in doing so, also to consider any admission of guilt (if given) in the light of other evidence taken. The Supreme Court also noted that the applicant had not put forward for consideration any other circumstance that might have raised doubt about Judge V.L.'s impartiality.

51. As regards the storage and use of the relevant telecommunications data, the Supreme Court noted that the data in question had been obtained on the basis of a court order issued under section 149.b of the CPA (see paragraph 57 below), which had not been declared invalid by the Constitutional Court. In the Supreme Court's view, the Constitutional Court's decision in question (see paragraphs 66-68 below) had not had an effect on the data collected and obtained by the authorities prior to its delivery. The Supreme Court furthermore noted that the Constitutional Court had not revoked the provision pursuant to which the obtained data was to be stored by the court for as long as the criminal file was maintained. The respective data had been obtained and stored more than three years before the delivery of the above-mentioned CJEU judgment and of the Constitutional Court's decision (see paragraphs 66-68 and 74-76 below). The Supreme Court went on to find that the accessing and processing of the data by the authorities had not amounted to an indiscriminate and preventive measure. The order to obtain the telecommunications data had been limited to a relevant period and had been based on the fact that there were grounds for suspicion that the applicant had committed the alleged crime, and on the incriminating facts and information which the authorities had had beforehand. It also observed that secret surveillance measures, such as wiretapping (which had to be based on a reasonable suspicion – a standard of proof stricter than the grounds for suspicion required for the granting of access to communications data), had been ordered against the applicant and that the subsequent order to obtain telecommunications data had therefore interfered to a lesser extent with his right to communication privacy. It concluded that the measures taken against the applicant had not disproportionately interfered with the applicant's right to communication privacy and protection of personal data (as guaranteed by the Constitution) and that there were therefore no reasons to find that the

impugned criminal proceedings had been conducted in a manner that had been in contravention of fundamental procedural rules.

D. The Constitutional Court's decision

52. The applicant lodged two constitutional complaints. He complained, *inter alia*, about the refusal to allow the examination of E.R. and M.S., which had allegedly violated his defence rights, and the non-recusal of Judge V.L. He furthermore complained that there had been no constitutionally permissible basis for the non-selective storage of telecommunications data by the relevant telecommunications service providers. The applicant reiterated and further elaborated the arguments that he had put forward when pursuing his previous remedies. He also pointed out the alleged discrepancy between the position of the Supreme Court during the criminal and disciplinary proceedings against him (see paragraph 47 above) and argued that the retention and processing of his telecommunications data should have not been assessed through the lens of section 149.b of the CPA, because that data had been retained unlawfully, under a regime that had been declared invalid owing to its disproportionate nature. Access to such data and its storage in the case file could not have transformed the unlawfully retained data into data that was compliant with the Constitution. He cited section 18 of the CPA, which provided that no court decision could be based on evidence that had been obtained in violation of constitutionally guaranteed human rights.

53. On 24 September 2018 the Constitutional Court accepted the applicant's constitutional complaints for consideration; on 9 October 2019 it dismissed them on the merits. With regard to the refusal of the request that M.S. and E.R. be examined, it found the lower courts' decisions convincing. In its view, it was crucial to note that E.R. had chosen to remain silent and that the applicant's conviction had not relied exclusively or decisively on M.S.'s statement.

54. With regard to the non-recusal of Judge V.L., the Constitutional Court held that the actions of the applicant's co-defendants (who had served as intermediaries in respect of the bribery) and the applicant (the person who had solicited the bribe) had originated in the same past event; in fact, those actions had entailed different forms of participation in the same criminal offence. The Constitutional Court considered it obvious that the intermediaries' actions had been connected to the actions of the official person (that is, the applicant) who had solicited or accepted a bribe, and that the latter's act had constituted a prerequisite for establishing the intermediaries' criminal responsibility and the existence of bribery. However, the judgment on the basis of E.R.'s and M.S.'s admission of guilt had only concerned the applicant's co-defendants (who had admitted their guilt). The Constitutional Court further noted that the epistemic value of an admission of guilt (that is to say its impact on the assessment of the case) depended on the

stage of the proceedings in question at which it was given: the later in the process of evidence gathering it was given, the lower the weight that it commanded in the judge's cognitive process. The co-defendants gave their admission of guilt only during the nineteenth hearing of the trial, when the evidence-taking had already entered its final stage and had nearly been completed. In the Constitutional Court's view, it could therefore not be considered that Judge V.L. had formed a preconceived opinion regarding the applicant's guilt because of his co-defendants' admission. Although the judgment – which had been based on E.R.'s and M.S.'s admission of guilt – had implied that Judge V.L. had been convinced of their guilt and had mentioned the role of the applicant, it had not referred to any opinion of the court regarding the applicant's guilt, and nor had the court in its judgment against the applicant referred to the co-defendants' admission of guilt. The Constitutional Court accordingly concluded that the applicant's right to have his case heard by an impartial judge had not been violated.

55. With regard to the storage and use of telecommunications data, the Constitutional Court noted that the data obtained in the applicant's case had allowed for conclusions to be drawn about the location, time, duration and type of communication – as well as information about "who called whom". The obtained data had allowed for detailed findings to be reached about the privacy of the applicant, co-defendants and the injured party. The Constitutional Court pointed out that both its previous decision and the CJEU's judgment in *Digital Rights Ireland and Others* (see paragraphs 66-68 and 74-76 below) had concerned the retention of data – not access to such data. Therefore, access to data could not be assessed through the criteria established in these respective decisions. The Constitutional Court went on to examine the proportionality of the interference with the applicant's communication privacy constituted by the authorities having access to his data. It found that in its orders granting access the first-instance court had established (as required by law) that there were grounds for suspecting that a criminal offence had been committed, and that access to the telecommunications data had been necessary for the investigation of the respective crime. It also noted that the applicant had not alleged that the conditions set out under section 149.b of the CPA for gaining access had not been fulfilled. The Constitutional Court went on to note that the criminal offence in question had related to corruption and had been of a serious nature. With respect to the question of the duration of the measure, the Constitutional Court considered the period in respect of which the data had been accessed by the authorities. It referred to the periods set out in section 107.a of the Amended 2004 Act, noting that that provision had been essentially the same as the provision under the 2012 Act (see paragraph 65 below) that had been declared invalid by the decision of 3 July 2014. It further noted that data could for a certain period be retained also in "commercial bases" under section 104 of the Amended 2004 Act (see paragraph 64 below). It went on to observe

that the telecommunications data in question had been obtained several years prior to the publication of its decision of 3 July 2014 (see paragraphs 66-68 below). Furthermore, even though the data obtained in the criminal proceedings against the applicant related to the above-stipulated period of fourteen months and the four analytical reports had at least indirectly incriminated the applicant, the Ljubljana District Court had referred to a narrow range of obtained data in corroborating E.Ć.'s testimony and dismissing the credibility of the applicant's defence. Those data had concerned specific telephone communications that had taken place only one month and four days before the first access order had been issued and two months before the last access order had been issued. The Constitutional Court therefore found it likely that the telecommunications data referred to directly in the first-instance court judgment had been stored during the period allowed for "commercial bases". According to the Constitutional Court, that fact was also significant for an assessment of the proportionality of the measure, as it reduced the weight of the encroachment on the applicant's rights. The Constitutional Court concluded that the other courts had properly justified the interference with the applicant's right to communication privacy and could not be criticised for failing to strike a reasonable balance between that right and the interests of the criminal proceedings.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. DOMESTIC LAW AND PRACTICE

A. Criminal Procedure Act

56. The Criminal Procedure Act, which came into force on 1 January 1995, with relevant amendments, provides in its section 39 (entitled "exclusion") as follows:

> "(1) A judge or lay judge may not perform judicial duties:
>
> ...
>
> 4) if he in respect of the same matter has [already] acted as a prosecutor, defence lawyer, ... [or] representative, or has been examined as a witness or an expert;
>
> 5) if he took part in adopting the lower court's decision in respect of the same matter or took part at the same court in adopting a decision [that was subsequently] challenged by an appeal or by an application for the protection of legality;
>
> 6) if circumstances exist that give rise to doubts regarding his impartiality."
>
> (2) A judge or lay judge may not decide on the charges ...:
>
> ...
>
> 3) if he has [already] issued a decision that the admission of guilt [in question] should be dismissed (under section 285.c(2)) or that the agreement on the admission of guilt should be dismissed ..."

57. Section 149.b, in the chapter regulating measures taken by the police in pre-trial proceedings, provided at the relevant time:

> "(1) If there are grounds for suspecting (*razlogi za sum*) that a criminal offence for which a perpetrator is prosecuted *ex officio* has been committed, is being committed or is being prepared or organised, and information on communication using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the reasoned request of the public prosecutor, order the operator of the electronic communications network to forward to him information on the participants, circumstances and facts of electronic communication traffic, such as: the number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data forwarded; and the place where the electronic communications service was performed.
>
> (2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, the substantiation of the reasoning, the time period for which the information is required and other important circumstances that warrant the use of the measure.
>
> (3) If there are grounds for suspecting that a criminal offence for which a perpetrator is prosecuted *ex officio* has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the [relevant] directory – as well as information regarding the time that the means of communication was or is in use [or] needs to be obtained in order to uncover this criminal offence or regarding the perpetrator thereof – the police may request that the operator of the electronic communications network provide them with that information, at their written request and even without the consent of the individual to whom the information refers.
>
> (4) The operator of electronic communications networks may not disclose to its clients or to a third party the fact that it has given certain information to the investigating judge (first subsection of this section) or the police (the preceding section), or that it intends to do so."

58. Section 285.c(1), which regulates pretrial hearings, provides that if the defendant admits his or her guilt, the presiding judge has to assess, *inter alia*, whether his or her admission of guilt has been made of his or her own free will, is unambiguous and is supported by other evidence in the case file. After that, the presiding judge shall render a decision accepting or rejecting the admission of guilt, and that decision cannot be challenged (section 285.c(2)). If the admission of guilt is accepted, the defendant cannot withdraw it. The sentence is rendered at the sentencing hearing. The judgment's reasoning in respect of the defendant's guilt shall be limited to the finding that the defendant confessed to the charges and that that confession was accepted by the presiding judge (sections 285.c(3), (5) and (6), and 285.č). Under section 330, those provisions are to be applied, *mutatis mutandis*, to an admission of guilt that is given and accepted during the trial.

59. Section 324(2), which concerns the hearing of a defendant, is worded as follows:

"(2) After the defendant has finished his statement, he may be questioned. The presiding judge shall first call on the prosecutor and then the defence counsel to put questions to the defendant. The injured party, legal representative, attorney, co-defendant and expert may ask the defendant direct questions only with the permission of the presiding judge."

60. Furthermore, section 326(1) reads:

"(1) After the questioning of the first defendant has finished, co-defendants, if any, may be questioned in turn. After [the questioning of] each [co-defendant] the presiding judge shall acquaint that co-defendant with the statements of any co-defendants who have been questioned before him and ask him if he has any comments in respect thereof, [and] and shall ask [any] co-defendant [who was] examined before him if he has any comments in respect of the statement of the subsequently examined co-defendant. Each defendant shall be entitled to put questions to other examined co-defendants."

61. Section 5(3) provides that a defendant shall not be obliged to defend himself or to answer any questions; if he decides to defend himself he shall not be obliged to give any statement that could incriminate him or his next of kin, or to confess his own guilt.

B. Criminal Code

62. Article 261 § 1 of the Criminal Code, which came into force on 1 November 2008, provides as follows:

Acceptance of a bribe

"(1) An official or a public officer who requests or agrees to accept for himself or any third person an award, gift or other property benefit, or a promise or offer of such a benefit, in return for carrying out an official act within the scope of his official duties that should not be performed (or not to carry out an official act that should or could be performed), or otherwise abuse his position, or whoever serves as an agent for the purpose of bribing an official, shall be sentenced to imprisonment for not less than one and not more than eight years and punished by a fine."

63. Article 54 sets out the condition under which a criminal offence is considered to be of a continuous nature (that is, considered to constitute a continuous criminal offence) and sentences that can be imposed in such a situation.

C. The Amended 2004 Act

64. The Electronic Communications Act was in force between 1 May 2004 and 14 January 2013. In so far as relevant, it was amended in 2006, in the part concerning the retention of data, with a view to transposing the Data Retention Directive (see paragraph 70 below); it was further amended in 2009 (hereinafter "the Amended 2004 Act "). It provided, in so far as relevant, as follows:

Section 104
(Traffic data)

"(1) Traffic data relating to subscribers and users processed and retained by an operator must be deleted or rendered anonymous as soon as they are no longer needed for the purpose of forwarding communications, except in the cases of categories of data from section 107.b of this Act, which are to be retained under subsections 4 and 5 of section 107.a of this Act.

(2) Without prejudice to the provision [set out under] the preceding section, an operator may, until complete payment for a service is made (but no later than by the expiry of the limitation period), retain and process traffic data required for the purposes of calculating and paying bills relating to interconnections.

(3) For the purposes of marketing electronic communications services or the provision of value-added services, the provider of the service [in question] may process the data referred to in the first subsection of this section to the extent and for the duration necessary for such services or marketing, but only if the subscriber or user to whom the data relates has given his prior consent. Subscribers or users must be informed (prior to their giving consent) of the types of traffic data that are processed and the duration of such processing. A user or subscriber shall have the right to withdraw [his or her] consent at any time.

(4) For the purposes referred to in the second subsection of this section, a service provider must state in [its] general terms and conditions which traffic data will be stored [and] processed and the duration of that processing, and they must further state that the data will be managed in accordance with the Act governing personal data protection.

(5) Traffic data may only be processed under the previous subsections of this section by persons acting under the authority of an operator and handling billing or traffic, responding to customer enquiries, detecting fraud, marketing electronic communications services or providing value-added services; ... such processing must be restricted to what is necessary for the purposes of such activities.

(6) Without prejudice to the provisions of the first, second, third and fifth subsections of this section, an operator shall send traffic data to the relevant body if that body so requests in order to settle disputes (in particular, interconnection or billing disputes), in accordance with the applicable legislation."

Section 107.a
(general provisions regarding the retained data)

"(1) Operators must, for the purpose of obtaining data on traffic in the public communications network (as stipulated by the Act governing criminal procedure) [and] for the purpose of ensuring national security, constitutional order and the security-related, political and economic interests of the state ... and the national defence ..., retain the data referred to in section 107.b of this Act if [such data] is generated or processed during the provision of related public communications services.

...

(3) The obligation referred to in the first subsection of this section shall also apply to the retention of data on unsuccessful call attempts, where that data is generated or processed or retained or recorded when ensuring related public communications services. This obligation shall not include the retention of data on connections that were not successfully established, and the content of communications.

...

(5) Operators shall ensure the retention of the data referred to in the first, third and fourth subsections of this section, in accordance with the provisions of this Act, for fourteen months from the day of communication (in respect of data related to publicly available telephone services) and eight months from the day of communication (in respect of other data).

(6) The ... body that decides on access to the data referred to in the first subsection ... may extend the period of retention for a limited period if this is required by particular circumstances relating to the criminal prosecution, ...

(7) Upon the expiry of the retention period, the operators should destroy all the data retained, in accordance with the provisions of this Act, except for those with respect to which an order to access such data has been issued or which have already been forwarded to the relevant authority."

Section 107.b
(data to be retained)

"Data that should be stored (hereinafter "the stored data") are as follows:

1. data required in order to trace, identify and recognise the source of communication, including:

- concerning fixed network telephony and mobile telephony: the telephone number of the caller, and the name and address of the subscriber or registered user;

- as regards [internet-related data] ...;

2. data required to identify the destination of a communication, including:

- concerning fixed network telephony and mobile telephony: the number dialled, ... the number to which the call is routed, [and] the name and address of the subscriber or registered user;

- as regards [Internet-related data]...;

3. data required to identify the date, time and duration of communication, including:

- concerning fixed network telephony and mobile telephony: the date and time of the start of the communication and the duration or the time of the end of the communication;

- as regards [Internet-related data]...;

4. data required to identify the type of communication, including:

- concerning fixed network telephony and mobile telephony: the telephone service used;

- as regards [Internet-related data]...;

5. data required to identify the users' communication equipment, including:

- concerning fixed network telephony: the number from which the call was made and the number called;

- concerning mobile telephony: the calling and called telephone numbers, the International Mobile Subscriber Identity of the calling party and of the called party, the International Mobile Equipment Identity of the calling party and the called party, [and] – with respect to prepaid anonymous services – the date and the time of the initial

activation of the service and the cell ID [that is, the label of the location] from which the service was provided;

- as regards [Internet-related data]...;

6. data required for the identification of the location of the mobile communication equipment [in question]:

- the location label (cell ID) at the start of communication;

- data identifying the geographical location of cells by reference to their location labels during the period for which the communications data was retained."

Section 107.c
(Protection of retained data)

"(1) Operators shall ensure that retained data is secured in accordance with the law governing the protection of personal data. In this respect, they shall, individually or jointly, take appropriate technical and organisational measures to protect retained data against destruction, loss or alteration and against unauthorised or unlawful forms of storage, processing, access or disclosure.

(2) Operators may process retained data only to the extent necessary to ensure their storage.

(3) Retained data shall be of the same quality as the data on the network. Retained data shall be subject to those provisions of this Act that concern the protection and safeguarding of the data on the network.

(4) The [mail and electronic communications] agency shall, after first obtaining the opinion of the Information Commissioner, prescribe in detail in a general regulation the manner in which data shall be stored and the method of implementation of this section."

Section 107.č
(Data access order and forwarding of the data)

"(1) The operator shall forward the retained data immediately, but at the latest within three days of receipt of a copy of the part of the order from the relevant authority that sets out all the necessary information concerning the scope of access.

...

(3) Upon receipt of the order, the operator shall forward the retained data to the relevant authority to the extent specified in the copy of the operative part of the order.

(4) Operators shall, together with the [those] authorities that may require access to the retained data, ensure that there is for a period of ten years an indelible record of each forwarding of the retained data and shall, within that period, store the data obtained and supplied from the date on which they were forwarded to the relevant authority and shall protect them in accordance with the ... order's designated confidentiality classification.

(5) The Minister shall, in agreement with the Minister responsible for the Internal Affairs, the Minister responsible for Defence and the Director of the Slovenian Intelligence and Security Agency, prescribe in detail the manner of the forwarding of the retained data."

Section 112
(oversight)

"...

(2) The Information Commissioner shall supervise the storage of traffic and location data obtained or processed in connection with ensuring public communications networks or services, in accordance with sections 107.a-e of this Act, and the forwarding of the data specified in section 104.a of this Act."

Section 142
(Cooperation between supervisory authorities)

"The Agency, the ... inspectors and the Information Commissioner have a duty to cooperate and inform each other of the supervisory measures taken, to provide each other with the information necessary for the implementation of the oversight and to cooperate professionally."

65. In 2012 the Amended 2004 Act was replaced by a new Act (namely, "the 2012 Act"), whose sections 163 and 164 contained the same provisions as those contained in section 107.a and section 107.b of the Amended 2004 Act.

D. Constitutional Court's decision U-I-65/13 of 3 July 2014

66. At the request of the Slovenian Information Commissioner, the Constitutional Court reviewed the constitutionality of the 2012 Act with respect to the retention of data – including its sections 163 and 164 (see paragraph 65 above). In its decision of 3 July 2014 the Constitutional Court, referring to the CJEU's judgement of 8 April 2014 (*Digital Rights Ireland and Others* – see paragraphs 74-76 below) revoked the respective provisions of the 2012 Act, finding that they were not in compliance with the right to protection of personal data.

67. The Constitutional Court found that the processing of personal data under the impugned provisions amounted to an interference with the right to protection of personal data (Article 38 § 1 of the Constitution). It further established that the aims pursued by the legislature – that is, *inter alia*, the prevention, investigation, and prosecution of serious crime – were permissible. In its view, the means employed were also suitable for achieving those aims. As regards the necessity of the interference, the Constitutional Court noted, *inter alia,* that the obligatory and non-selective retention of traffic data encroached on the rights of many people who were not and would never be in any way linked to the purposes for which the data was collected. In particular, the legislation in question did not limit the retention of data to a certain period of time or geographical area, or to a circle of persons who could have a certain link with the purposes pursued by the measure. The legislature also failed to justify why the duration of the retention of the data in question (fourteen or, in some cases, eight months) was necessary.

Moreover, the legislature did not set out the specific criminal offences with respect to which the retention of data would be justified.

68. Noting the serious nature of the interference and finding that the legislature had failed to limit the scope of measure to that which had been necessary in order to achieve the objectives pursued, the Constitutional Court concluded that the impugned provisions disproportionally interfered with the right to the protection of personal data and were unconstitutional. It annulled the impugned provisions and ordered that the data retained on the basis of those provisions be immediately destroyed. On 10 November 2022 a new Electronic Communications Act came into force. It does not provide the general retention of telecommunications data for purposes other than those related to the provision of commercial services.

II. EUROPEAN UNION LAW AND PRACTICE REGARDING PROTECTION OF DATA AND PRIVACY

A. Relevant EU law

69. Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union ("the Charter") provide as follows:

Article 7 – Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 – Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

Article 11 – Freedom of expression and information

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

70. The domestic legal provisions on data retention (see paragraphs 64-65 above), which are the subject of the applicant's complaints, transposed Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services

or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54) (hereinafter "the Data Retention Directive"). That directive laid down the obligation on providers of publicly available electronic communications services or of public communications networks to retain certain data that had been generated or processed by them, in order to ensure that they would be available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member State in its national law. The Data Retention Directive applied to traffic and location data and to any related data that was necessary to identify the subscriber or registered user in question. It did not apply to the content of electronic communications (Article 1). Article 3 set out the obligation to retain data specified in Article 5 (which was transposed in section 107.b of the Amended 2004 Act – see paragraph 64 above). Article 6 stipulated that such data were to be retained for periods of not less than six months and not more than two years from the date of the communication in question. Under Article 8 of the Data Retention Directive, member States were required to ensure that that data was retained in such a way that they (and any other related necessary information) could be forwarded upon request to the relevant authorities without undue delay.

71. The Privacy and Electronic Communications Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("the E-Privacy Directive") – consolidated in the text version of 19 December 2009, which combines the initial act and subsequent amendments made thereto in accordance with Directive 2009/136/EC of 25 November 2009, and its Corrigendum 2009/136 of 10 September 2013) contains specific provisions designed to offer to the users of electronic communications services protection against risks to their personal data and privacy that arise from new technology and from the increasing capacity for automated storage and for the processing of data (recitals 5 to 7 of that directive). Article 5(1) provides that member States must ensure the confidentiality of communications effected by means of a public communications network and publicly available electronic communications services, and the confidentiality of the related traffic data. It also provides that all persons other than the users are prohibited from, *inter alia*, storing – without the consent of the users concerned – traffic data relating to electronic communications, except when legally authorised to do so under Article 15(1). The latter provision sets out the conditions for derogations from the principle of confidentiality, allowing member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive in the event that such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society for the purpose of safeguarding national security (that is, State security) defence and

public security, and the prevention, investigation, detection and prosecution of criminal offences or of the unauthorised use of the electronic communication system. It stipulates that to this end, member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period on specific grounds and that such measures shall conform with the general principles of Community law – including those referred to in Articles 6 § 1 and 2 of the Treaty on European Union.

72. Under Article 6 of the E-Privacy Directive, traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly-available electronic communications service must be erased or rendered anonymous when it is no longer needed for the purpose of the forwarding of a communication. Furthermore, the processing of traffic data is permitted for the billing and marketing of services and the provision of value-added services under specific conditions. As regards the billing of services, such processing is permitted only up until the end of the period during which the bill may be lawfully challenged, or legal proceedings brought in order to obtain payment. As regards location data other than traffic data, Article 9 § 1 of that directive provides that that data may be processed only subject to certain conditions and only after it has been rendered anonymous or the consent of the users or subscribers has been obtained to the extent and for the duration necessary for the provision of a value added service.

73. In respect of the General Data Protection Directive and the Law-Enforcement Directive, see *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, §§ 234-39, 11 January 2022.

B. Relevant case-law of the Court of Justice of the European Union

1. Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238)

74. Following requests for a preliminary ruling (which had originated in an action brought by the Irish Company Digital Rights Ireland in the High Court in Ireland and several constitutional actions brought in the Austrian Constitutional Court), the CJEU assessed the validity of the Data Retention Directive – in particular, in the light of Article 7 and Article 8 of the Charter. On 8 April 2014 (see paragraph 66 above for the full reference) the CJEU ruled that the Data Retention Directive was invalid.

75. The CJEU observed that the data which communication providers were obliged to retain on the basis of the Data Retention Directive, taken as a whole, might allow very precise conclusions to be drawn concerning the private lives of those persons whose data had been retained. The following passages are particularly relevant in this respect:

> "26 In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks

must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27 Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."

The CJEU further found that by providing for the retention and processing of personal data, the Data Retention Directive constituted a wide-ranging and particularly serious interference with the rights guaranteed by Articles 7 and 8 of the Charter. Referring to *Leander v. Sweden* (26 March 1987, § 48, Series A no 116), *Rotaru v. Romania* ([GC], no. 28341/95, § 46, ECHR 2000-V), and *Weber and Saravia v. Germany* ((dec.), no. 54934/00, § 79, ECHR 2006-XI), the CJEU noted that the access of the relevant national authorities to such data constituted a further interference with the rights protected by Article 7 of the Charter. It observed that the fact that data were retained and subsequently used without the subscriber or registered user being informed was likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance.

76. As regards the justification for the interference, the CJEU noted that the impugned Directive did not permit the acquisition of knowledge of the content of the communications as such and required that the data retention be accompanied by certain data security measures. The interference did not therefore affect in essence the rights guaranteed by Articles 7 and 8 of the Charter. After finding that the data retention for the purpose of allowing the relevant national authorities to possibly have access to those data genuinely satisfied an objective that was in the general interest (namely, the fight against serious crime), it went on to examine the proportionality of the interference. In this connection the CJEU reached, *inter alia*, the following conclusions:

"49 As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

...

54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99).

55 The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

...

57 In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59 Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1 § 1, in a general manner to serious crime, as defined by each member State in its national law.

61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. ...

62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on member States designed to establish such limits.

63 Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64 Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66 Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. ...

...

69 Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter."

2. Tele2 Sverige and Watson and Others (C-203/15 and C-698/15, EU:C:2016:970)

77. In a judgment of 21 December 2016 (pursuant to requests for a preliminary reference lodged by the Administrative Court of Appeal of Stockholm, Sweden, and the Court of Appeal of England and Wales), the referring courts raised, *inter alia*, the question of whether a general and indiscriminate obligation to retain electronic communications data was *per se* incompatible with Articles 7 and 8 and Article 52 § 1 of the Charter, or whether the compatibility of such retention of data was to be assessed in the

light of provisions relating to access to data, the protection and security of data and the duration of their retention. The CJEU clarified that while the member States could adopt (in line with Article 15 § 1 of the E-Privacy Directive) legislative measures providing for the retention of traffic and location data, such retention of data was to constitute an exception and not the rule. In this connection it found that Article 15 § 1 of that Directive, read in the light of Articles 7, 8 and 11 and Article 52 § 1 of the Charter, did not prevent a member State from adopting legislation permitting (as a preventive measure) the targeted retention of traffic and location data for the purpose of fighting serious crime; however, such retention of data was limited – with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted – to what was strictly necessary. In particular, the retention of data had to meet objective criteria that established a connection between the data to be retained and the objective pursued. Such conditions must be shown actually to circumscribe, in practice, the extent of that measure and thus the public affected. The CJEU further noted:

> "111 ... As regards the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence that makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to fighting serious crime or to prevent a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."

3. La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791)

78. In a judgment of 6 October 2020, given pursuant to requests for a preliminary reference lodged by the French Council of State and the Belgian Constitutional Court, the CJEU referred, *inter alia*, to the findings in the above-cited judgments and clarified that the retention of traffic and location data constituted, in itself, on the one hand, a derogation from the prohibition laid down in Article 5 § 1 of the E-Privacy Directive, and, on the other, an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter – irrespective of whether the information in question relating to private life was sensitive or whether the persons concerned had been inconvenienced in any way on account of that interference. It also noted that whether or not the retained data had been used subsequently was irrelevant in that connection. In the 6 October 2020 judgment the CJEU specifically addressed the objective of safeguarding national security and found that the importance of that objective went beyond that of the other objectives referred to in Article 15 § 1 of Directive 2002/58, and could therefore justify a legislative measure that permitted the relevant authorities to order providers

of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time, as long as there were sufficiently solid grounds for considering that the member State concerned was confronted with a serious threat to national security – which the CJEU further defined, and which had to have been shown to be genuine and present or foreseeable. However, even that retention could not be systematic in nature and had to be subject to review either by a court or an independent administrative body.

79. The CJEU also found that member States were not precluded from adopting legislative measures aimed at combating serious crime (and, *a fortiori*, at safeguarding national security) by means of issuing an instruction (pursuant to a decision issued by the relevant authority, which would be subject to effective judicial review) requiring providers of electronic communications services to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers. It noted that in order to ensure that the interference constituted by a measure of that kind was limited to that which was strictly necessary, (i) the retention obligation should relate only to traffic and location data that might shed light on serious criminal offences or actions adversely affecting national security, and (ii) the duration for which such data was retained had to be limited to that which was strictly necessary – although that duration could be extended where the circumstances and the objective pursued by that measure justified doing so. It further noted that such expedited retention did not need to be limited to the data of persons specifically suspected of having committed a criminal offence or acts adversely affecting national security; rather, it might be extended to traffic and location data relating to persons other than those who were suspected of having planned or committed a serious criminal offence or acts adversely affecting national security – provided that that data could, on the basis of objective and non-discriminatory factors, shed light on such an offence or such acts.

80. As regards the limits on the temporal effect of the declaration of illegality with respect to general and indiscriminate retention of traffic and location data and the use in the criminal proceedings of evidence obtained as a result of such retention, the CJEU concluded as follows:

> "228 ... a national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Article 15 § 1 of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52 § 1 of the Charter. Article 15 § 1 interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context

> of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact."

81. As regards the admissibility of evidence, the CJEU reiterated that under EU law it was in principle for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of information and evidence obtained by such retention of data contrary to EU law.

4. Prokuratuur (C-746/18, EU:C:2021:152)

82. A judgment of 2 March 2021, given pursuant to a request for a preliminary reference lodged by the Supreme Court of Estonia, originated in proceedings in which H.K. was found guilty of, *inter alia*, several thefts, on the basis of, *inter alia*, evidence obtained from a communications services provider. The investigating authority obtained traffic and location data concerning H.K.'s telephone numbers and International Mobile Equipment Identity codes (which had been retained for a duration of one year by the said providers) in a pre-trial procedure after being granted several authorisations for that purpose by the relevant prosecutor's office. The CJEU reiterated that Article 15 § 1 of the E-Privacy Directive permitted access to retained telephone traffic or location data for the purpose of fighting crime only when the crime in question was serious or presented a serious threat to public security. Moreover, the CJEU noted that Article 15 § 1 applied regardless of the length of the period in respect of which access was sought and the quantity or nature of the data available in respect of that period. As regards the admissibility of evidence, the CJEU referred to *Quadrature du Net and Others*, noting as follows:

> "44 In deciding whether to exclude information and evidence obtained in contravention of the requirements of EU law, regard must be had, in particular, to the risk of breach of the adversarial principle and, therefore, of the right to a fair trial entailed by the admissibility of such information and evidence. If a court takes the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and that is likely to have a preponderant influence on the findings of fact, it must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an infringement. Therefore, the principle of effectiveness requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority thereto in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact (see, to that effect, judgment of 6 October 2020, La

Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 226 and 227)."

83. The CJEU went on to hold that the power to examine access requests could not be given to a prosecutor's office, since its tasks of directing pretrial proceedings and prosecuting affected its independence *vis-à-vis* parties to criminal proceedings.

5. *Commissioner of An Garda Síochána and Others (C-140/20, EU:C:2022:258)*

84. A judgment of 5 April 2022 was given pursuant to a request for a preliminary reference lodged by the Supreme Court of Ireland. It related to proceedings in which G.D., who had been convicted for murder, sought a declaration that certain provisions of the domestic law (namely provisions requiring the retention of traffic and location data and allowing the disclosure of such data when required for, *inter alia*, the prevention, detention, investigation and prosecution of a serious offence) were invalid, with a view to contesting, as part of the criminal proceedings, the admissibility of that evidence. The CJEU noted that criminal behaviour – even of a particularly serious nature – could not be treated in the same way as a threat to national security. Traffic and location data could not therefore be the object of general and indiscriminate retention for the purpose of combating serious crime; accordingly, access to such data could not be justified for that same purpose. It reiterated that only the targeted retention of traffic and location data and the expedited retention of such data under the conditions set out in *La Quadrature du Net and Others* were permissible (paragraphs 78 to 80 above). It explained that member States had the option of imposing retention measures targeting persons who, on the basis of an identification, were (i) the subject of an investigation or other surveillance measures or (ii) noted in the national criminal record as having been convicted of a serious crime and presenting a high risk of reoffending; the CJEU added that where an identification was based on objective and non-discriminatory factors that were defined in national law, targeted retention in respect of persons thus identified was justified. It further explained that the relevant national authorities were not precluded from ordering a measure of expedited retention during the first stage of an investigation into a serious threat to public security or a possible serious crime – that is, from the time when the authorities might, under the provisions of national law, commence such an investigation.

85. As regards the relevant authorities having access to retained traffic and location data, the CJEU reiterated that such access had first to be reviewed by a court or by an independent administrative body and that the decision of that court or body had to be delivered following a reasoned request by those authorities that was lodged, *inter alia*, within the framework of procedures aimed at the prevention, detection or prosecution of crime. The

CJEU found that a police officer in the legal system under consideration, who had been authorised to carry out a prior review of requests for access to data, had not fulfilled the requirements of independence and impartiality.

86. As regards the effect of the interpretation of the E-Privacy Directive and the Charter upheld in its previous judgments in *Tele2 Sverige and Watson and Others* and *La Quadrature du Net and Others*, the CJEU reiterated that, according to settled case-law, the interpretation that the Court gave to a rule provided by EU law – within the exercise of the jurisdiction conferred upon it by Article 267 of the Treaty on the Functioning of the European Union – clarified and defined the meaning and scope of that rule as it should be, or ought to have been, understood and applied from the time of its coming into force. In the CJEU's view, the rule as thus interpreted might and should be applied by the courts to legal relationships that had arisen and had been established before the delivery of a ruling on the request for interpretation – but only provided that in other respects the conditions for bringing an action relating to the application of that rule before the courts having jurisdiction were satisfied. As regards the admissibility of evidence relied on against G.D. the CJEU referred to the principle of the procedural autonomy of the EU member States and to the principles set out in *Prokuratuur*.

6. SpaceNet and Telekom Deutschland (C-793/19 and C-794/19, EU:C:2022:702)

87. Lastly, a judgment of 20 September 2022 was given pursuant to a request for a preliminary reference lodged by the German Federal Administrative Court and concerned the question of whether the member States were precluded from adopting a national legislative measure which, with certain exceptions, required electronic communications services providers – for the purposes set out in Article 15 § 1 of the E-Privacy Directive, and, *inter alia*, for the purposes of prosecuting serious criminal offences or preventing a specific risk to national security – to retain, in a general and indiscriminate way, most of the traffic and location data of the end users of those services, laying down a retention period of several weeks and rules intended to ensure the effective protection of the retained data against the risks of abuse and against any unlawful access to those data. The CJEU found that the data retention obligation at issue could not be regarded as constituting a targeted retention of data and that the duration of the retention of traffic and location data (ten weeks and four weeks respectively) – albeit short – had enabled precise conclusions to be drawn concerning the private lives of those concerned and had amounted to serious interference with their privacy. It also found that the national legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 regarding access to retained data could not, by its very nature, be capable of either limiting or even remedying the serious interference that will result from the general retention of such data. The CJEU emphasised in that

connection that as regards the safeguards provided by the national legislation that were at issue in the main proceedings (which were intended to protect retained data against the risks of abuse and against any unlawful access), each instance of such data being retained and accessed constituted a separate interference with the fundamental rights guaranteed by Articles 7 and 11 of the Charter, and each such instance required a separate justification under Article 52 § 1 of the Charter.

88. In that judgment the CJEU also addressed the Court's case-law, which had been cited by certain governments in respect of similar cases; it observed that the judgments in *Big Brother Watch and Others v. the United Kingdom* ([GC], nos. 58170/13 and 2 others, 25 May 2021) and *Centrum för rättvisa v. Sweden* ([GC], no. 35252/08, 25 May 2021) could not call into question its interpretation of Article 15 § 1 of Directive 2002/58 regarding the general and indiscriminate retention of traffic and location data. It noted that in those judgments the Court had been concerned with the bulk interception of data relating to international communications and had not ruled on the compatibility with the Convention of an instance of the general and indiscriminate retention of traffic and location data on national territory or even the large-scale interception of such data for the purposes of the prevention, detection and investigation of serious criminal offences. The CJEU went on to observe that Article 52 § 3 of the Charter was intended to ensure the necessary consistency between the rights set out in the Charter and the corresponding rights guaranteed by the ECHR, without adversely affecting the autonomy of EU law and that of the CJEU; consequently, for the purposes of interpreting the Charter, account should be taken of the corresponding rights of the ECHR only as the minimum threshold of protection.

THE LAW

I. PRELIMINARY REMARKS

89. The Court notes that in his reply to the Government's observations the applicant raised a new argument concerning Judge V.L.'s alleged bias owing to her having been acquainted with certain evidence that had been excluded from the criminal-case file. In the Court's view, the new argument raised by the applicant is not an elaboration of the original complaint which he lodged with the Court on 21 April 2020 and of which the Government were given notice. Mentioned only incidentally, it does not contain sufficient factual and legal basis to qualify as a "complaint" within the meaning of the Court's case-law (see *Radomilja and Others v. Croatia* [GC], nos. 37685/10 and 22768/12, § 126, 20 March 2018). The Court will therefore not examine it.

II. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

90. The applicant complained of the first-instance court's refusal to allow the examination of E.R. and M.S. as witnesses at the trial. He also complained that the judge of the court that had convicted him could not be considered impartial, given her role in the proceedings against E.R. and M.S. and the content of the judgment against them that she had delivered. He relied on Articles 6 §§ 1 and 3 (d) of the Convention, which reads as follows:

> "1. In the determination of ... any criminal charge against him, everyone is entitled to a fair ... hearing ... by [a] ... tribunal ...
>
> ...
>
> 3. Everyone charged with a criminal offence has the following minimum rights:
>
> ...
>
> (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
>
> ..."

A. Admissibility

91. The Court notes that this part of 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' arguments

92. The applicant argued that an examination of M.S. and E.R. would have served to corroborate his defence – namely his attempt to prove that he had never demanded or received payment from E.Ć. and that the money that he had received from M.S. had been in fact given to him in repayment of a loan. Neither of the two defendants, who had been alleged intermediaries in the offence allegedly committed by the applicant, had stated before making their respective admissions of guilt that the applicant had demanded money from them. M.S. had moreover not said why he had given EUR 8,000 to the applicant. However, this could have been clarified had the applicant been given the possibility of questioning M.S. Furthermore, the covertly recorded communications, on which the judgment had extensively relied, had concerned M.S. and E.R. The district court had interpreted those communications to the detriment of the applicant while the latter had been unable to clarify their content by examining M.S. and E.R.

93. The applicant further argued that after M.S. and E.R. had confessed, he should have been given the opportunity to confront them. He submitted

that (contrary to the findings of the domestic courts) the judgment against him had cited M.S.'s statement, as well as referring to that statement when rejecting the applicant's defence regarding the repayment of the above-mentioned loan. As regards the argument that M.S. and E.R. could not have been examined on account of their status as defendants, the applicant argued that the domestic court could have simply adjourned the proceedings in order to wait for the judgment against them to become final. He pointed out that it had become final a day after the applicant had been convicted. As to the Government's argument that the applicant had not asked to be allowed to question the co-defendants, the applicant argued that he would not in any case have been in a position to compel them to answer questions since they had decided to remain silent and had been protected by the privilege against self-incrimination. He also pointed out that when M.S. had given his statement during the investigation, neither the applicant nor his representative had been given the opportunity to be present.

94. The applicant also submitted that once Judge V.L. had had accepted E.R.'s and M.S.'s admission of guilt she had no longer appeared to be impartial. For her to convict E.R. and M.S. she had to have assessed the case in substance, and the fact that she had found them guilty meant that she must have considered that the applicant was guilty as well. That was why she had subsequently rejected all applications requesting that evidence be taken and had proceeded to deliver the judgment finding the applicant guilty.

95. The Government submitted that the actions of E.R. and M.S. as intermediaries in bribery had been dependent on the fact that the applicant had demanded or accepted the bribe in question. They considered it important that their admissions of guilt had been made almost at the end of the proceedings, and that the judgment against the applicant had not referred to E.R.'s and M.S.'s respective admissions of guilt.

96. As regards the dismissal of the applicant's request that E.R. and M.S. be examined, the Government pointed out that E.R. had not wished to defend himself in the proceedings and that M.S. had been willing to speak in his own defence only when heard by the investigating judge. The applicant had commented on M.S.'s statement but had never asked to be allowed to put questions to M.S. The Government further submitted that the impugned judgments had referred to M.S.'s statement only in support of the factual findings made on the basis of other produced evidence; referring to the findings of the domestic courts, they argued that an examination of M.S. and E.R. had not been warranted, given the circumstances of the case.

2. The Court's assessment

(a) Refusal to allow the examination of E.R. and M.S.

(i) Preliminary remark

97. The Court notes that the applicant alleged that his right under Article 6 § 1 and 6 § 3 (d) had been violated because the trial judge (Judge V.L.) had refused to allow the examination of E.R. and M.S. The Court further notes that Article 6 § 3 (d) enshrines the right of a defendant to examine or have examined witnesses against him as well as the right to call witnesses for the defence. Since the principles relevant to the examination of the compliance of the domestic proceedings with Article 6 § 3 (d) differ in some aspects (see *Al-Khawaja and Tahery v. the United Kingdom* [GC], nos. 26766/05 and 22228/06, §§ 118-47, ECHR 2011, and *Schatschaschwili v. Germany* [GC], no. 9154/10, §§ 110-31, ECHR 2015, as regards prosecution witnesses; see also *Murtazaliyeva v. Russia* [GC], no. 36658/05, §§ 150-68, 18 December 2018, as regards defence witnesses), the Court considers it necessary to clarify whether the applicant's grievance relates to the examination of prosecution witnesses or the right to call witnesses for the defence. In this connection, the Court observes that it has so far not specified the criteria for distinguishing the two categories of witnesses within the context of Article 6 § 3 (d).

98. In the present case the applicant in his submissions before the domestic courts referred to E.R. and M.S. sometimes as witnesses against him (see paragraph 32 above) and sometimes as witnesses for the defence (see paragraph 34 above). In order to determine whether his complaint concerns, in substance, the right of a defendant to examine or have examined witnesses against him or the right to call witnesses for the defence, the Court has to look at the reasons adduced for his request to have the witnesses in question examined. It observes that M.S. gave a statement during the investigation, when neither the applicant nor his lawyer appear to have been present and thus able to observe and react to it. However, by calling him as a witness the applicant did not seem to want to seek only to test the rather limited statement that M.S. had given during the investigation. The applicant requested that E.R. and M.S. be heard with a view to establishing that they had acted on their own, that he (that is, the applicant) had never received the initial payment and that he had believed that the money that he had received from M.S. had constituted the repayment of a loan that he had made to the latter. In the Court's view, the arguments that the applicant advanced before the domestic courts and in the proceedings before the Court (see paragraphs 29-32, 43, 46, 92 and 93, above) indicate that his request for the examination of E.R. and M.S. was essentially meant to support his defence against the criminal charges that he faced. In view of the foregoing – and noting that E.R. did not testify in the proceedings and that the judgment against the applicant did not refer to the statements that E.R. and M.S. had

given within the context of their admissions of guilt – the Court will consider the applicant's complaint under Articles 6 §§ 1 and 3 (d) from the perspective of the right to call witnesses on behalf of the defence.

(ii) General principles

99. The Court reiterates that under Article 6 of the Convention the admissibility of evidence is primarily a matter for regulation by national law and that the Court's task is not to give a ruling as to whether statements of witnesses were properly admitted as evidence, but rather to ascertain whether the proceedings as a whole (including the way in which evidence was taken) were fair (see, among many other authorities, *Van Mechelen and Others v. the Netherlands*, 23 April 1997, § 50, *Reports* 1997-III, and *Perna v. Italy* [GC], no. 48898/99, § 29, ECHR 2003-V). Article 6 § 3 (d) of the Convention does not require the attendance and examination of every witness on the accused's behalf; rather, the essential aim of that provision (as indicated by the words "under the same conditions") is to ensure a full "equality of arms" in respect of the matter in question (see *Engel and Others v. the Netherlands*, 8 June 1976, § 91, Series A no. 22; *Vidal v. Belgium*, 22 April 1992, § 33, Series A no. 235-B; and *Murtazaliyeva*, cited above, §139).

100. In *Murtazaliyeva* (cited above, § 158) the Court formulated the following three-pronged test for an assessment of whether the right to call a witness for the defence under Article 6 § 3 (d) has been complied with: (1) whether the request that a witness be examined was sufficiently reasoned and relevant to the subject matter of the accusation; (2) whether the domestic courts considered the relevance of that testimony and provided sufficient reasons for their decision not to allow the examination of a witness at trial; and (3) whether the domestic courts' decision not to allow the examination of a witness undermined the overall fairness of the proceedings.

101. In respect of the first element the Court has held that it is necessary to examine whether the testimony of witnesses was capable of influencing the outcome of a trial or could reasonably be expected to strengthen the position of the defence. The "sufficiency" of reasoning of the requests lodged by the defence requesting that witnesses be examined will depend on the assessment of the circumstances of the case in question, including the applicable provisions of the domestic law, the stage and progress of the proceedings, the lines of reasoning and strategies pursued by the parties and their procedural conduct (ibid., §§ 160-61).

102. As to the second element of the test, the Court has explained that generally the relevance of testimony and the sufficiency of the reasons advanced by the defence in the circumstances of the case will determine the scope and level of detail of the domestic courts' assessment of the need to ensure a witness' presence and examination. Accordingly, the stronger and weightier the arguments advanced by the defence, the closer must be the scrutiny and the more convincing must be the reasoning of the domestic

courts if they refuse the defence's request for the examination of a witness (ibid., § 166).

103. With regard to the assessment of overall fairness (the third element of the test), the Court stressed in the case of *Murtazaliyeva* that compliance with the requirements of a fair trial must be examined in each case, having regard to the development of the proceedings as a whole and not on the basis of an isolated consideration of one particular aspect or one particular incident. While the conclusions under the first two steps of that test will generally be strongly indicative of whether the proceedings were fair, it cannot be excluded that in certain (admittedly exceptional) cases considerations of fairness might warrant the opposite conclusion (ibid., §§ 167-68).

(iii) Application of the principles to the present case

104. The Court notes that the applicant and the two co-defendants (E.R. and M.S.) were tried together until 11 December 2013 (the day of the nineteenth hearing – see paragraphs 27 and 54 above). By that point extensive evidence had been taken, but neither the applicant nor E.R. or M.S. had actively defended themselves. When, on 11 December 2013, E.R. and M.S. pleaded guilty, Judge V.L. accepted their respective admissions of guilt. The applicant consequently requested that Judge V.L. be excluded from the proceedings against him on account of her alleged lack of impartiality, but to no avail. Two days later, on 13 December 2013, Judge V.L. disjoined the proceedings against E.R., and M.S. and on 16 December 2013 she convicted them of the continuous offence of assisting in the bribery of the applicant. At the hearings in the proceedings (which now concerned only the applicant) held on 13 and 19 December 2013, the applicant made a defence statement. He also requested that E.R. and M.S. be examined as witnesses and that the proceedings be adjourned until this became possible (see paragraphs 32 and 34 above). Judge V.L. dismissed his request with the explanation that the judgment against E.R. and M.S. was not final (meaning they could not yet be examined as witnesses) and that sufficient evidence had been put forward to allow her to decide on the charges against the applicant. On 23 December 2013 Judge V.L. found the applicant guilty of the continuous offence of accepting a bribe. Two days later the judgment against E.R. and M.S. became final (see paragraphs 24-37 above).

105. The Court observes that in his request for the examination of E.R. and M.S., submitted through his representative, the applicant argued, *inter alia*, that: M.S. might be able to provide information concerning the loan to which the applicant referred in his defence statement; E.R. might be able to testify about E.Ć.'s debts to him; and that he would prove that E.R. and M.S. had not told him that they had requested money on his behalf. He argued that that E.R. and M.S. were no longer co-defendants in the same proceedings and could be examined as witnesses (see paragraphs 29-32 above). The Court further observes that: the applicant's conviction was founded largely upon

evidence relating to conversations between M.S., E.R., E.Ć. and the applicant, which the domestic court was called upon to interpret within the given context; E.Ć.'s recorded testimony regarding the initial events was inconsistent (see paragraphs 10, 21 and 41 above); and M.S. and E.R. – who were alleged to have played a crucial role in facilitating the applicant in committing the alleged offence – were not heard during the trial. Given the initial status of M.S. and E.R. as defendants and their wish not to defend themselves (see paragraph 25 above), the Court does not find of any particular relevance the fact that the applicant did not lodge a request for them to be called as witnesses before they were convicted (see paragraph 96 above).

106. In view of the above-noted considerations the Court is not convinced that the applicant's request for M.S. and E.R. to be called as witnesses was not sufficiently founded or was not relevant to the subject-matter of the accusations against him. In other words, it does not consider that any testimony given by M.S. and E.R. would not have been capable of influencing the outcome of the trial or could not have been reasonably expected to strengthen the position of the defence (see *Murtazaliyeva*, cited above, §§ 160-61).

107. As regards the second element of the *Murtazaliyeva* test (see paragraph 102 above), the Court notes that Judge V.L. gave certain reasons for her dismissal of the application for E.R. and M.S. to be examined (see paragraphs 33-34 above). Firstly, Judge V.L. noted that she did not base her assessment of the evidence on M.S.'s and E.R.'s admission of guilt. However, as stated above, the applicant requested, at least in substance, that M.S. and E.R. be called on behalf of his defence. The fact that the prosecution had not based their arguments on the admissions of guilt given by M.S. and E.R. could not be seen as important in this respect. The same goes for the argument that the applicant's conviction did not rely exclusively or decisively on M.S.'s statement (see paragraph 53 above). In respect of the fact that the domestic courts referred to the fact that the applicant had given his defence statement only later in the proceedings (see paragraphs 33, 34, 48 and 53 above), the Court notes that the applicant did not change his account of events but rather gave it only after M.S. and E.R. had confessed. It is not for the Court to speculate why he decided to pursue this defence strategy, but in any event, this was his right and there is nothing suggesting that his conduct could be considered as constituting an attempt to abuse his procedural rights.

108. Secondly, as regards the domestic courts' argument that M.S. and E.R. could have not been examined because the judgment against them was not final (in other words, at that point they were still co-defendants – see paragraphs 33, 34, 48 and 53 above), the Court finds that reasoning unpersuasive, given the circumstances of the case. It observes that Judge V.L. was clearly aware of the eight-day deadline for M.S. and E.R. to declare their intention to appeal (see paragraph 36 above). She, being the ultimate guardian of the fairness of the proceedings, was expected to carefully measure the

consequences of her procedural decisions on the applicant's defence rights (see, *mutatis mutandis*, *Kikabidze v. Georgia*, no. 57642/12, § 59, 16 November 2021). While of course she could not speculate at that point as to whether M.S. and E.R. would avail themselves of the possibility to appeal, nothing seems to have prevented her from adjourning the hearing in order that the said short (eight-day) deadline would expire – particularly given that the judgment against M.S. and E.R. was based on their admission of guilt, so there was a reasonably small chance that they would appeal against it. The Court therefore finds that the domestic courts failed to provide sufficient reasons for refusing to call M.S. and E.R. as witnesses.

109. Lastly, as regards the overall fairness of the proceedings, the Court notes that it appears that the testimony of M.S. and E.R. would have been important, given that they were the only witnesses who could confirm or deny the version of events put forward by the applicant in his defence statement (see paragraphs 29-32 above). In view of the development of the proceedings it could not have been anticipated at the stage in question how M.S. and E.R. would respond to the applicant's version of events had they been summoned to testify. It likewise cannot be presumed that had this evidence been produced it would have had no impact on the outcome of the trial. The fact that the applicant was deprived of the opportunity to effectively adduce witness evidence and to rely on it in arguing his case therefore rendered the trial proceedings unfair.

110. In view of the above-noted considerations, the Court concludes that the criminal proceedings against the applicant were not compliant with Article 6 §§ 1 and 3 (d) of the Convention. The domestic courts that dealt with the remedies pursued by the applicant did not redress this shortcoming.

111. There has accordingly been a violation of Article 6 §§ 1 and 3 (d) of the Convention.

(b) Alleged lack of impartiality of Judge V.L.

112. The Court considers that in view of the above-mentioned finding of a violation of Article 6 §§ 1 and 3 (d) of the Convention, it is not necessary to examine whether Article 6 § 1 was also violated on account of Judge V.L.'s alleged lack of impartiality (see paragraph 90 above).

III. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

113. The applicant complained that the retention of the telecommunications data relating to his telecommunication activities and its use in the proceedings against him had been in breach 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

114. 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' arguments

115. The applicant submitted that the relevant provisions of the Amended 2004 Act and of the 2012 Act, which had been repealed by the Constitutional Court, had been identical. Relying on the judgment of the CJEU (see paragraphs 74-76 above) and the Constitutional Court's decision of 3 July 2014 (see paragraphs 66-68 above), he argued that the storage of the data in question had been in violation of Article 8 *ab initio,* and that as a result, their acquisition and use had also been in breach of the Constitution and the Convention. In this respect he also referred to a discrepancy between the findings of the Supreme Court in the criminal proceedings, on the one hand, and the findings reached in the disciplinary proceedings, on the other (see paragraph 47 above). He furthermore argued that section 149.b of the CPA (see paragraph 57 above) should have limited the possibility to access retained data to only serious offences.

116. Furthermore, in the applicant's submission, given that the data obtained in his case had been tainted by the unconstitutionality of the legislation pursuant to which it had been retained, it should not have been used as evidence in his trial. The applicant also argued that a distinction should not have been made between the data obtained, respectively, prior to and after the respective Constitutional Court decision (see paragraphs 66-68 above). This distinction had amounted to unequal treatment. Data storage that amounted to a violation of his right to privacy could not be *ex post* validated by the courts in specific proceedings by way of finding that the storage in question had in fact been proportionate. The applicant also pointed out that section 149.b of the CPA (see paragraph 57 above) had not constituted the basis for the data retention but rather the basis for obtaining the retained data. As regards the Constitutional Court's reference to "commercial bases" with respect to the storage of data (see paragraph 55 above), the applicant submitted that this argument had been based on a mere possibility and had not amounted to a finding that the storage had in fact been lawful.

117. The Government, who in their observations mainly reiterated the findings of the Constitutional Court (see paragraphs 66-68 above), argued that in the present case the data had been obtained from the telecommunications providers lawfully, on the basis of the then valid relevant legislation. They pointed out that the provisions of the Amended 2004 Act underpinning the storage of the applicant's data had not been invalidated with *ex tunc* effect. While the measure in question had allowed detailed inferences to be made about the private lives of those concerned (namely, the intensity, location, time and duration of communication between E.R., M.S., E.Ć. and the applicant), it had been necessary in view of the nature of the alleged crime and the public interest involved. Reasons for suspicion that the criminal offence of bribery was being committed had been sufficiently justified. The Government also pointed out that the Constitutional Court, which had later invalidated the impugned legal provisions, had not ordered that the data in question (which had by then been obtained by the courts) be destroyed. Moreover, the legal basis for the retention of the data in question could also be found in section 104(2) of the Amended 2004 Act, which had allowed for data retention for commercial purposes. Lastly, the Government was of the view that the telecommunications data had not been stored nor meant for use in disciplinary proceedings and that the related evidence had therefore been rightly excluded from the case file relating to those proceedings (see paragraph 47 above).

2. The Court's assessment

(a) Relevant principles and case-law

118. The Court has already established that subscriber, traffic and location data can relate – alone or in combination – to the "private life" of those concerned (see *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 372, 11 January 2022). It has furthermore consistently found that the mere retention of data relating to someone's private life amounts to an interference with that individual's right to respect for his or her "private life" (ibid.; see also *Breyer v. Germany*, no. 50001/12, § 81, 30 January 2020, and *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, § 244, 25 May 2021). It amounts also to an interference with the right to respect for the correspondence of the individual concerned (see *Ekimdzhiev and Others*, cited above, § 373, and *Ben Faiza v. France*, no. 31446/12, §§ 66-67, 8 February 2018). The subsequent use of stored data has no bearing on that finding (see *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II, and *Trajkovski and Chipovski v. North Macedonia*, nos. 53205/13 and 63320/13, § 51, 13 February 2020). However, access by the authorities to retained data constitutes a further interference with the right to respect for one's private life and one's communications under Article 8 of the Convention (see *Ekimdzhiev and Others*, cited above, § 376; see also, *mutatis mutandis*, *Centrum för*

rättvisa, cited above, § 244, and *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, § 330, 25 May 2021).

119. The Court reiterates that in view of the technological and social developments in the sphere of electronic communications, communications data can nowadays reveal a great deal of personal information. If obtained by the authorities in bulk, such data can be used to paint an intimate picture of a person through, *inter alia*, the mapping of social networks, location tracking, mapping of communication patterns, and insight into who that person has interacted with (see *Centrum för rättvisa*, § 256, and *Big Brother Watch and Others*, § 342, both cited above). The acquisition of such data through bulk interception can therefore be just as intrusive as the bulk acquisition of the content of communications, which is why their interception, retention and search by the authorities must be analysed by means of reference to the same safeguards as those applicable to content (see *Centrum för rättvisa*, § 277, and *Big Brother Watch and Others*, § 363, both cited above). This finding applies also to the general retention of communications data by communications service providers and its access by the authorities in individual cases, which must be accompanied, *mutatis mutandis*, by the same safeguards as those pertaining to secret surveillance (see *Ekimdzhiev and Others*, cited above, § 395).

120. Any interference with an individual's Article 8 rights 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 that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 227, ECHR 2015, and *Kennedy v. the United Kingdom*, no. 26839/05, § 130, 18 May 2010). In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question of whether the "necessity" test has been complied with; it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society" – in particular by providing adequate and effective safeguards and guarantees against abuse (see *Roman Zakharov*, § 236; *Kennedy*, § 155; and *Big Brother Watch and Others*, § 334, all cited above).

121. On a general note, as regards the protection of personal data, the Court held in *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 103, ECHR 2008, as follows:

> "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article .... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data

> are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and 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 (see Article 5 of the Data Protection Convention ... [in paragraph 47 above]). The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention [in paragraph 47 above]) ..."

122. Principles governing the question of when surveillance measures (including the interception of communications) can be justified under Article 8 § 2 of the Convention were set out in detail in *Roman Zakharov* (cited above, §§ 227-34, 236, 243, 247, 250, 257-58, 275, 278 and 287-88). Those principles were recently adapted within the context of bulk interception in *Centrum för rättvisa* (cited above, §§ 246-53 and 262-64) and *Big Brother Watch and Others* (cited above, §§ 332-39 and 348-50).

123. With respect to the bulk interception of data relating to international communications, the Court has considered that the degree of interference with individuals' Article 8 rights increases as the process progresses (*Big Brother Watch and Others*, cited above, § 325). It has however observed that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (ibid., § 330). In that regard, the Court has found it imperative that when a State is operating a bulk-interception regime, domestic law should set out detailed rules regarding when the authorities might resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised. Moreover, as defined in previous case-law, the domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed (ibid., § 348; see also *Centrum för rättvisa*, cited above, § 262). Within the same context the Court has found that to minimise the risk of the bulk interception being abused, the process must be subject to "end-to-end safeguards" – meaning that (i) at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken, (ii) bulk interception should be subject to independent authorisation at the outset, when the object and scope of the bulk operation are being defined, and (iii) the operation should be subject to supervision and independent *ex post facto* review (see *Big Brother Watch and Others*, § 350, and *Centrum för rättvisa*, § 264, both cited above).

124. As to the question of whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aims of, *inter alia*, protecting national security or preventing and prosecuting criminal offences. However, this margin is subject to

European supervision embracing both legislation and decisions applying it, and considering all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by national law (see *Roman Zakharov*, § 232, and *Breyer*, § 79, both cited above).

(b) The Court's assessment of the present case

(i) Scope of the examination

125. The Court observes that the traffic and location data (hereinafter also "communications data" – or, where specific to telephony, "telecommunications data") related to the applicant were in the present case obtained by the law-enforcement authorities pursuant to court orders that were based on grounds for suspicion that the applicant (who was at the time a judge) had been involved in bribery – that is, in a criminal offence of a serious nature. It further notes that – except for the scope of the access orders, which was not limited to serious offences (see paragraph 115 above) – nothing was put forward to question the adequacy of the court orders or the legal framework within which they were issued. The issue that raises concerns with respect to Article 8 in the present case is, however, the regime underpinning the collocation of telecommunications data from which those relating to the applicant were obtained for the purposes of the criminal proceedings against him. In order to ascertain whether the interference constituted by that retention was "in accordance with the law" and proportionate, the Court must assess the Slovenian law governing data retention that was in force at the time in question.

126. The Court notes that the applicant's telecommunications data, like those of any other user of telecommunications services, was at the time retained pursuant to section 107.a of the Amended 2004 Act, which transposed the relevant provisions of the Data Retention Directive (see paragraph 64 above). The aforementioned provision required electronic communications providers to retain for a period of fourteen months, *inter alia*, communications data relating to fixed and mobile telephony for a number of purposes – namely for the purposes of criminal procedure and of ensuring national security, constitutional order, and the security, political and economic interests of the State and of the national defence. It must be emphasised that the applicant's data was not retained for the specific purpose of preventing or investigating serious crime but for any of the aforementioned purposes. The interference with his Article 8 rights constituted by the retention of his data must therefore be assessed within this broader context.

127. Having said that, the data in question were accessed and processed in the criminal proceedings against the applicant, which prompted his complaint. In the criminal proceedings the domestic courts, including the

Constitutional Court, substantially assessed the matter that is now before the Court.

(ii) Existence of an interference

128. It has not been disputed in the present case that the retention of the applicant's telecommunications data and the access to and processing of such data by the authorities amounted to interferences with his rights protected by Article 8 of the Convention. The Court, having regard to its case-law (see paragraph 118 above), sees no reason to find otherwise. It further finds that the interference concerning the data retention by the communications service providers was required by law and was thus attributable to the Slovenian State (see *Ekimdzhiev and Others*, cited above, § 375).

129. The Court must now examine whether the interference was justified in terms of Article 8 § 2 of the Convention – that is, whether it was in accordance with the law, pursued a legitimate aim and was "necessary in a democratic society".

(iii) Justification for the interference

(α) "In accordance with the law"

130. It is common ground between the parties that at the relevant time the retention of telecommunications data had a sufficiently clear legal basis in the Amended 2004 Act (see paragraph 64 above) and was therefore foreseeable. Access to such data was authorised by the Ljubljana District Court's orders issued on the basis of section 149.b of the CPA (see paragraphs 12-17 and 57 above). In this connection, it is to be noted that the court orders appeared to specify a longer period than that authorised by law. However, the respective service provider stored the data only for the statutory period of fourteen months and handed over to the authorities only such (that is, up to fourteen-months-old) data (see paragraph 17 above). The interference in question was thus in this respect compliant with the domestic law, as in force at the time in question. That said, the Court notes that after the telecommunications data had been obtained in the applicant's case, the Constitutional Court (see paragraphs 66-68 above) – relying on the CJEU's judgment in *Digital Rights Ireland and Others* (see paragraphs 74-76 above) – found that the data retention regime under the 2012 Act (which was in this respect essentially the same as that under the Amended 2004 Act) breached the privacy rights of the users of electronic communications services. The Court will take this into consideration when examining the "necessity" of the interference, which is closely related to "lawfulness" in this type of cases (see paragraph 120 above).

(β) Legitimate aim

131. It has not been disputed that the data retention regime under consideration pursued the legitimate aims set out in the second paragraph of Article 8. The Court finds that the retention regime in question could be considered to have pursued the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, or the protection of the rights and freedoms of others. The accessing and processing of the telecommunications data relating to the applicant could be considered to have pursued the legitimate aims of preventing crime and protecting the rights and freedoms of others.

(γ) "Necessary in a democratic society"

– *Level of interference*

132. The present case does not concern a direct interception of data by the authorities, although it does relate to the risks of such interception. Under the impugned legal provisions, service providers were legally required to collect and store telecommunications data (beyond the extent necessary for billing or other contractual purposes) in order to have them available for the authorities. Most of these data were likely never consulted. In this respect the case is comparable to that of *Breyer* (cited above), where the interference complained of consisted of the service providers' legal obligation to collect and store personal details of users of pre-paid mobile SIM cards (together with the accompanying telephone numbers), with a view to making such data available to the authorities upon request (ibid., §§ 76-77).

133. However, unlike the case of *Breyer*, which concerned an interference of a limited nature (ibid., § 95), the present case concerns telecommunications data (see section 107.b of the Amended 2004 Act, cited in paragraph 64 above) which, when linked to a subscriber or a user, can reveal intimate pictures of his or her life through the mapping of social networks, location tracking, the mapping of communication patterns, and insight into who they have interacted with (see *mutatis mutandis*, *Ekimdzhiev and Others*, § 394; *Centrum för rättvisa*, § 256; and *Big Brother Watch and Others*, § 342, all cited above). In the Court's view, the systemic surveillance entailed by the mandatory retention of telecommunications data presents an impediment to the enjoyment of the privacy rights of all users of telecommunication services. The existence of large collections of telecommunications data and the ongoing retention of such data could understandably generate a sense of vulnerability and exposure and could prejudice persons' ability to enjoy privacy and the confidentiality of correspondence, to develop relations with others and to exercise other fundamental rights. In this regard the Court also refers to the observations made by the CJEU in *Digital Rights Ireland and Others* – namely, that communications data, taken as a whole, might allow "very precise conclusions to be drawn concerning the private lives of the

persons whose data had been retained", and that its retention and processing therefore constituted "a wide-ranging and particularly serious interference" with their fundamental rights (see paragraph 76 above). The severity of the interference was acknowledged also by the respondent Government (see paragraph 117 above) and the Slovenian Constitutional Court (see paragraphs 55 and 66-68 above).

134. In view of the above-noted considerations, the Court finds that the interference constituted by the data retention under consideration was of a serious nature. It must now determine whether the means provided under the impugned legislation for the achievement of the legitimate aims (see paragraph 131 above) complied with the requirements of the principle of the rule of law and remained in all respects within the bounds of what was necessary in a democratic society.

– *Breadth of the margin of appreciation*

135. Although this point has not been demonstrated by any empirical data, the Court has no doubt that the tracing of telecommunications traffic – which was enabled by the retention duty provided in the impugned legislation – could be of considerable importance for effective law enforcement and effective public security measures. It reiterates that the fight against crime (in particular, organised crime and terrorism, which constitutes one of the challenges faced by today's European societies), upholding public safety and the protection of citizens constitute "pressing social needs" (see *Breyer*, cited above, § 88). It also recognises that modern means of telecommunications and changes in communication behaviour require that investigative tools for law enforcement and national security agencies be adapted (see *S. and Marper*, cited above, § 105).

136. That said, for an interference to be compliant with the second paragraph of Article 8 it does not suffice that it is capable or effective in advancing the aim in question; it also needs to be proportionate in the sense that it strikes a fair balance between the competing public interests and the rights enshrined in the Convention (see *Handyside v. the United Kingdom*, 7 December 1976, § 48, Series A no. 24; *Breyer*, cited above, § 91; and *Szabó and Vissy v. Hungary*, no. 37138/14, § 55, 12 January 2016). Admittedly, within a context of protecting national security or preventing and prosecuting criminal offences, national authorities enjoy a certain margin of appreciation when choosing the means of achieving a legitimate aim (see paragraph 124 above). However, this margin remains subject to review by the Court and its breadth depends on a number of factors dictated by the particular case. The margin will tend to be more narrow where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights or where the interference is far-reaching (see *S. and Marper*, cited above, § 102; also compare *Dubská and Krejzová v. the Czech Republic* [GC], nos. 28859/11 and 28473/12, § 178, 15 November 2016; *Dudgeon v. the United Kingdom*,

22 October 1981, § 52, Series A no. 45; and *National Union of Rail, Maritime and Transport Workers v. the United Kingdom*, no. 31045/10, §§ 86-87, ECHR 2014). Accordingly, having regard to the nature and severity of the interference at stake, the Court must exercise a correspondingly stricter scrutiny when assessing the question of fair balance (including the requisite safeguards) in the present case (contrast *Breyer*, cited above, §§ 94-96 and 103).

– *Assessment of "fair balance"*

137. The Court notes that while the legal provisions governing the treatment of communications data might be different from those governing the surveillance of the content of communication, they should be analysed with reference to the same safeguards as those applicable to the content itself (see, *mutatis mutandis, Big Brother Watch and Others*, cited above, § 416). Therefore, the general retention of communications data by communications service providers and its access by the authorities in individual cases must be accompanied, *mutatis mutandis*, by the same safeguards as secret surveillance (*Ekimdzhiev and Others*, cited above, § 395). In its case-law on surveillance measures within the context of criminal investigations, the Court has developed the following minimum safeguards, which should be set out in law in order to avoid abuses of power: the nature of offences that may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI, and *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008). In *Roman Zakharov* (cited above, § 231) – which concerned, in addition, other public-interest aims, such as the protection of national security – the Court framed the applicable safeguards along similar lines, with further emphasis placed on the notification mechanisms and the remedies provided by national law. It based its assessment of the compliance of the interception measures in question with Article 8 on the following criteria: the accessibility of the relevant domestic law; the scope and duration of the secret surveillance measures; the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data; the authorisation procedures; the arrangements for supervising the implementation of secret surveillance measures; and any notification mechanisms and the remedies provided by national law (ibid., § 238). Within the context of bulk interception relating to international communications, in *Big Brother Watch and Others* (cited above, § 361) and *Centrum för rättvisa* (cited above, § 275), the Court further adjusted the aforementioned criteria – including the requirement that the domestic law clearly define the grounds on

which bulk interception may be authorised, the circumstances in which an individual's communications may be intercepted and the procedure to be followed for granting authorisation.

138. As regards the present case, the Court observes that the Amended 2004 Act required, for several public-interest purposes, the retention for a period of fourteen months of all communications data generated or processed during the provision of related public communications services (see paragraph 64 above). The law did not seem to leave any decision in this respect to the discretion of any State or non-State body and was not ambiguous as to its application. Every individual or entity using the services of the telecommunications providers in Slovenia could anticipate that their telecommunications data was being retained as part of extensive data collection. However, the unambiguity of the law, which set out as a rule the general and indiscriminate retention of telecommunications data, could not be taken as constituting a sufficient guarantee of its compliance with the principles of rule of law and proportionality.

139. The Court observes that in *Ekimdzhiev and Others* (cited above), which concerned a similar regime governing the retention of communications data, it focused on the safeguards relevant to access to the retained data and the storage of accessed data; it did not pronounce on the compliance of the retention regime as such with the requirements of Article 8 (ibid., §§ 394-421). However, in the present case the applicant specifically complained of the retention of telecommunications data and the subsequent use of data that had been allegedly retained in breach of Article 8 (see paragraphs 125 and 126 above). The Court notes in this connection that the Amended 2004 Act set out a number of purposes for which the telecommunications data was to be retained, but it contained no provisions circumscribing the scope and application of the measure in relation to that which was necessary to achieve those purposes. Neither has it been shown that any other legislative act contained such provisions. It follows from the above-cited case-law (see paragraphs 119-123 and 137 above) that the national law should, as part of the minimum requirements, in a manner suitable to the particular form of surveillance, define the scope of application of the measure in question and provide appropriate procedures for ordering and/or reviewing it with a view to keeping it within the bounds of what is necessary. Having regard to the nature of the interference at issue (see paragraphs 132-134 above), those minimum requirements should have been met also by a measure entailing the retention of telecommunications data. The absence of provisions or mechanisms aimed at ensuring that the measure was actually limited to what was "necessary in a democratic society" for the specific purposes listed in the Amended 2004 Act rendered such a regime irreconcilable with the State's obligations under Article 8. The mere limitation of the retention to fourteen months, which is a considerable period, cannot undermine this conclusion.

140. The Court notes that the CJEU came to a similar conclusion in its judgment in *Digital Rights Ireland and Others*, which assessed the data retention regime in its entirety – that is, with respect to both the retention of telecommunications data and certain data relating to the Internet. The CJEU found that the regime of mandatory general and indiscriminate retention of communications data for the purposes of combating serious crime failed to comply with the requirement of proportionality (see paragraphs 74-76 above; see also the CJEU's findings in subsequent judgments clarifying and further developing the requirements, which are summarised in paragraphs 77, 78, 82, 84 and 87 above). Likewise, the Constitutional Court in its decision of 3 July 2014 (see paragraphs 66-68 above) declared the provisions governing the retention of communications data in the 2012 Act (which were essentially the same as those in the Amended 2004 Act) invalid. It referred to the aforementioned CJEU judgment. In its subsequent jurisprudence, the CJEU clarified that even within the context of safeguarding national security, where the retention of communications data could, under certain conditions, be ordered as a general and indiscriminate measure, such retention could not be systemic in nature and, when ordered, must be subject to independent review (see paragraph 78 above).

141. As regards the applicant's particular situation, the Court notes that it has not been disputed that the telecommunications data relating to the applicant was at the relevant time retained – in a systemic, general and indiscriminate manner – under the Amended 2004 Act. These data – stored for the period of fourteen months – were acquired by the authorities for the purposes of a criminal investigation being undertaken against the applicant. They were then processed, which resulted in analytical reports that were lodged in the applicant's criminal file. When dismissing his privacy-related complaints, the domestic courts referred to the fact that (i) the data in question had been accessed before the regime in question had been declared invalid, and (ii) the court orders authorising the accessing of the data had been based on the suspicion that a serious crime had been committed and were justified by the proportionality of the measure (see paragraphs 45, 51 and 55 above). The Constitutional Court also opined that the telecommunications data referred to in the judgment convicting the applicant related to the short period in respect of which the data could have been obtained from the "commercial bases" (see paragraph 55 above).

142. In respect of these considerations, the Court deems that the fact that the retention regime was declared invalid by the CJEU and the Constitutional Court after the data in question had been accessed could not be taken to mean that it had complied with Article 8 at the material time. What is important is whether at the time that his telecommunications data was retained, the applicant enjoyed the legal protection to which he was entitled under the Convention. In view of the findings and considerations set out in paragraphs 137-140 above, the Court considers that this was not the case.

143. The Court further notes that despite the applicant having clearly argued that the telecommunications data relating to his telecommunications had been retained in breach of his privacy rights, the domestic courts limited their assessment almost exclusively to the grounds on which the judicial orders had authorised access to the retained data – even though those grounds (as noted by the Constitutional Court) had not been challenged by the applicant (see paragraph 55 above). The Court would emphasise in this connection that even though the access to his data was accompanied by certain safeguards (such as judicial oversight), these safeguards, while being among the criteria that must be met (see *Ekimdzhiev and Others*, cited above, §§ 360-421), were not in themselves sufficient to render the retention regime compliant with Article 8. It notes by way of comparison that the CJEU similarly held in *SpaceNet and Telekom Deutschland* that national legislation that ensured full respect for the conditions established by its case-law interpreting the Data Retention Directive regarding access to retained data could not, by its very nature, be capable of either limiting or even remedying a serious interference resulting from the general retention of such data, the retention of and access to such data being separate interferences requiring separate justifications (see paragraph 87 above).

144. The applicant also argued that on account of the unjustified retention of his data, their acquisition and use in the domestic proceedings had violated Article 8 (see paragraphs 115 and 116 above). In this connection, the Court considers that when the retention of telecommunications data is found to violate Article 8 because it does not respect the "quality of law" requirement and/or the principle of proportionality, access to such data – and its subsequent processing and storage by the authorities – could not, for the same reason, comply with Article 8. In this connection, reference may again be made to the view expressed by the CJEU. In *An Garda Síochána and Others* the CJEU found that communications data could not be the object of general and indiscriminate retention for the purpose of combating serious crime and that therefore, access to such data could not be justified for that same purpose (see paragraph 84 above). The Court sees no reason to find otherwise in respect of the applicant's case.

145. The Court notes that a violation occurred in the present case, regardless of whether the data retained in breach of the applicant's Article 8 rights were cited by the domestic courts in finding the applicant guilty (see the principles referred to in paragraph 118 above and in *Huvig v. France*, 24 April 1990, § 35, Series A no. 176-B, where the impugned telephone tapping in question had not served as a basis for the prosecution). In this connection, the Court understands that the domestic courts' assessment of the impugned measures – including that conducted by the Constitutional Court (see paragraph 55 above) – was closely linked to the question of admissibility of evidence thus obtained (compare *Dragojević v. Croatia*, no. 68955/11, §§ 99 and 100, 15 January 2015). This is not surprising because it was carried

out within the context of the criminal proceedings against the applicant and was thus limited to the objective of those proceedings (see paragraph 127 above). However, for the purposes of Article 8, it is not of any particular significance that in convicting the applicant in the instant case, the domestic courts cited the limited range of the telecommunications data in question, which concerned a period of a month or so and which could have been kept for contractual purposes (see paragraph 55 above). The applicant's complaint concerned the entire set of his data relating to a period of fourteen months, which had been acquired by the law-enforcement authorities and then processed, kept and examined for the purposes of the criminal proceedings in question. It was not disputed that such a quantity of data could not and had not been kept for contractual purposes but had rather been retained as part of a general and indiscriminate retention regime, which the Court has found above to be in breach of Article 8 of the Convention.

146. Lastly, bearing in mind that the findings regarding the applicant's complaint under Article 8 do not concern the admissibility of evidence obtained against the applicant, which is a matter to be considered by the domestic courts in line with the applicable domestic legislation, the Court reiterates that the admission and use in judicial proceedings of evidence obtained in breach of Article 8 does not necessarily lead to the finding of a violation of Article 6 (see *Bykov v. Russia* [GC], no. 4378/02, §§ 89-91, 10 March 2009, with further references).

– *Conclusion*

147. In view of the above-noted considerations, the Court finds that the impugned provisions of the Amended 2004 Act, which were the basis for the retention of the applicant's telecommunications data, did not meet the "quality of law" requirement and were incapable of limiting the "interference" with the applicant's Article 8 rights to what was "necessary in a democratic society". The retention, access and processing of these telecommunications data were therefore in breach of Article 8 of the Convention.

IV. APPLICATION OF ARTICLE 41 OF THE CONVENTION

148. 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

149. The applicant claimed, in respect of non-pecuniary damage, 15,000 euros (EUR) for the violation of Article 6 of the Convention and EUR 5,000 for the violation of Article 8 of the Convention – a total of EUR 20,000. He further claimed around EUR 655,000 in respect of pecuniary damage arising from the loss of his job and thus income, the criminal fine imposed on him and the payment of a sum that amounted to the pecuniary gain realised from the committed crime (see paragraph 42 above).

150. The Government considered that the claim in respect of non-pecuniary damage was excessive. They also objected to the claim in respect of pecuniary damage and argued that the claim relating to loss of income was unfounded. They submitted that the applicant, if successful in the proceedings before the Court, would be able to request a reopening of the criminal proceedings. In their view, the finding of a violation should thus be considered to constitute sufficient just satisfaction.

151. The Court cannot speculate about what the outcome of the trial would have been had it been in conformity with Convention and notes that, as confirmed by the Government, the applicant will be able to request the reopening of the proceedings before the domestic courts. It thus rejects the applicant's claim for pecuniary damage. On the other hand, it accepts that the events leading to the violations found in the present case caused the applicant non-pecuniary damage that cannot be made good by the mere finding of a violation. The Court, making its assessment on an equitable basis, awards the applicant EUR 5,000 in respect of non-pecuniary damage, plus any tax that may be chargeable.

B. Costs and expenses

152. The applicant also claimed EUR 6,928 (including VAT) for the costs and expenses incurred before the Court and EUR 14,960 for those incurred during the proceedings before the domestic courts.

153. The Government argued that the claim for costs relating to the domestic proceedings was entirely unsupported. It argued that the claim in respect of the proceedings before the Court was excessive.

154. 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 notes that the applicant did not substantiate its claim related to the proceedings before the domestic courts. As regards the proceedings before the Court, it considers it reasonable to award the sum of EUR 5,000 covering costs under all heads, plus any tax that may be chargeable to the applicant.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 6 §§ 1 and 3 (d) of the Convention as regards the applicant's right to call witnesses for the defence;

3. *Holds* that there is no need to examine the merits of the complaint under Article 6 § 1 of the Convention as regards the impartiality of the trial judge;

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

5. *Holds*
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts at the rate applicable at the date of settlement:
      (i) EUR 5,000 (five thousand euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
      (ii) EUR 5,000 (five thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period, plus three percentage points;

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

Done in English, and notified in writing on 15 February 2024, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Liv Tigerstedt Deputy Registrar	Alena Poláčková President